

WORK PROCESS CONTROL GUIDE



*EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, ID
83415*

April 1979

UNITED STATES
DEPARTMENT OF ENERGY
DIVISION OF OPERATIONAL AND ENVIRONMENTAL SAFETY

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Available from:

System Safety Development Center
EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415

WORK PROCESS CONTROL GUIDE

Prepared By

M. G. Bullock

April 1979

ACKNOWLEDGMENTS

Special acknowledgment is given to Dr. R. J. Nertney for his technical direction and to my co-workers for their assistance. Special thanks to Della Kellogg for her editorial assistance and to Joann Walker for drafting the work process control tree.

FOREWORD

The purpose of this Guide is to identify the elements necessary in the development and evaluation of the ingredients that make up the work process. It defines the interrelationships between people, plant, and procedures. Also, it provides managers, supervisors, and safety specialists with concepts, information, and techniques to use in establishing and maintaining adequate worksite control.

The analytical tree is designed to set down, in a logical manner, factors which need consideration in a work process system. The tree is to be used in the conventional manner when analyzing an existing system. That is, one considers each element of the tree and makes judgments as to whether the element under consideration is adequate or less than adequate in maintaining adequate worksite control.

It is realized that some of the identified work process elements merit more detail or even books written about them. However, it is hoped that the ideas presented in this Guide will inspire the reader to do some creative thinking which will produce the needed job-related information.

CONTENTS

	<u>Page</u>
ACKNOWLEDGMENTS	i
FOREWORD	ii
I. INTRODUCTION	1
II. THE WORK PROCESS CONTROL TREE	8
1.0 ESTABLISH PERSONNEL REQUIREMENTS	8
1.1 Establish Personnel Selection Process.	9
1.2 Provide Personnel Training Process.	9
1.3 Establish Testing and Qualification Process.	10
1.4 Establish Process for Evaluating Current Status of Personnel.	11
2.0 ESTABLISH PLANT AND HARDWARE REQUIREMENTS	12
2.1 Provide Initial Conception and Design Requirements	12
2.2 Conduct Life Cycle Study	15
2.3 Provide Fabrication Control	16
2.4 Provide Installation Control	17
2.5 Establish Occupancy-Use Readiness Control.	17
2.6 Establish Adequate Operational Control.	18
2.7 Establish Change, Field Adjustment, or Modification Control.	21
2.8 Provide Decommission and Disposal Control	22
3.0 ESTABLISH PROCEDURE AND MANAGERIAL CONTROL REQUIREMENTS	23
3.1 Establish Managerial Control	23
3.2 Establish Procedure Requirements	24
III. CONCLUSION	26
IV. REFERENCES	28
APPENDIX A DESIGN REVIEW CRITERIA	29
APPENDIX B CRITERIA FOR PREPARATION OR REVIEW OF PROCEDURES	34

FIGURES

	<u>Page</u>
1. Plant-people-procedure relationships	3
2. The work process control tree	4
3. The work process schematic	6
4. The hardware schematic	13
5. The summary of job safety analysis	20
6. The application of system controls	27

I. INTRODUCTION

It is the common nature of almost all managers, when a piece of work goes sour, to immediately begin to focus their attention on the worksite location. They ask all the right questions to determine what happened when things started to go wrong, but very few questions are asked about what went wrong in the management system that allowed the situation to occur. Without examining the management system, the symptoms are often treated, rather than diagnosing and curing the causes of accidents. For example^[1], note the natural cycle when the lights in a home suddenly go out. Usually the appropriate fuse is replaced. If the new fuse blows, it too can be replaced. This process can be repeated endlessly, but it does not solve the basic electrical problem. Something is wrong with the electrical system when fuses fail repeatedly. The defect must be traced to the source of the trouble and corrected. Of course, there are those who would put a penny behind a fuse and let the house burn down.

Likewise, if a finger is lost because of an unguarded machine, the obvious thing to do is to have the machine guarded. But a guard (or fuse) promptly installed at the scene of an accident does not solve the "systemic" trouble. Why was the machine not guarded when purchased? Or, what is wrong with the day-to-day inspection plan that permits this unguarded condition to go unnoticed? Or, where did job orientation fail, since the employee did not report the deficiency? These and other questions stem from management deficiencies and cannot be attributed to the safety function. Note that each question relates back to a particular management function embracing a directive, a policy, or an organizational practice over which the immediate supervisor or the employee may have had no direct control.

It is this very logic which leads to the fact that "adequate worksite control and safety cannot be achieved unless we have a high quality of upstream processes which produce the worksite ingredients; namely, the people, the plant and hardware, and the procedures and management controls "[2]. There are several schools of thought about what constitutes adequate worksite control. These approaches are called the F syndrome because of the use of F words. One school says, Fit the person to the job, while another claims that the Form, Fit, and Function of the equipment must be controlled, and still another insists that Formal procedures are the answer. While all three of these approaches are important, they are not mutually exclusive. They each make up an integral part of the work process "system". By "system" we mean all of the people, plant, and procedure relationships that exist at the worksite. Figure 1 depicts this system including the necessary interfaces to ensure adequate worksite control.

The work process control tree, as shown in Figure 2, is a graphical representation of the necessary and sufficient elements needed to establish and maintain adequate worksite control. The summation gate at the top of the tree shows that the following tasks must be sufficiently performed in appropriate degrees to control any activity:

- 1.0 Establish Personnel Requirements
- 2.0 Establish Plant and Hardware Requirements
- 3.0 Establish Procedure and Managerial Control Requirements

For example, in the design of a gun, there is one end of the gun that cannot be made perfectly safe. Therefore, the control of the gun rests with the procedures and managerial controls placed on its use, along with the requirements of good construction and maintenance. Also, it rests with the people allowed to have guns. This example again points out the fact that the adequate worksite control is a combination of adequate personnel, plant and hardware, and procedural and managerial controls.

PLANT - PEOPLE - PROCEDURES RELATIONSHIPS

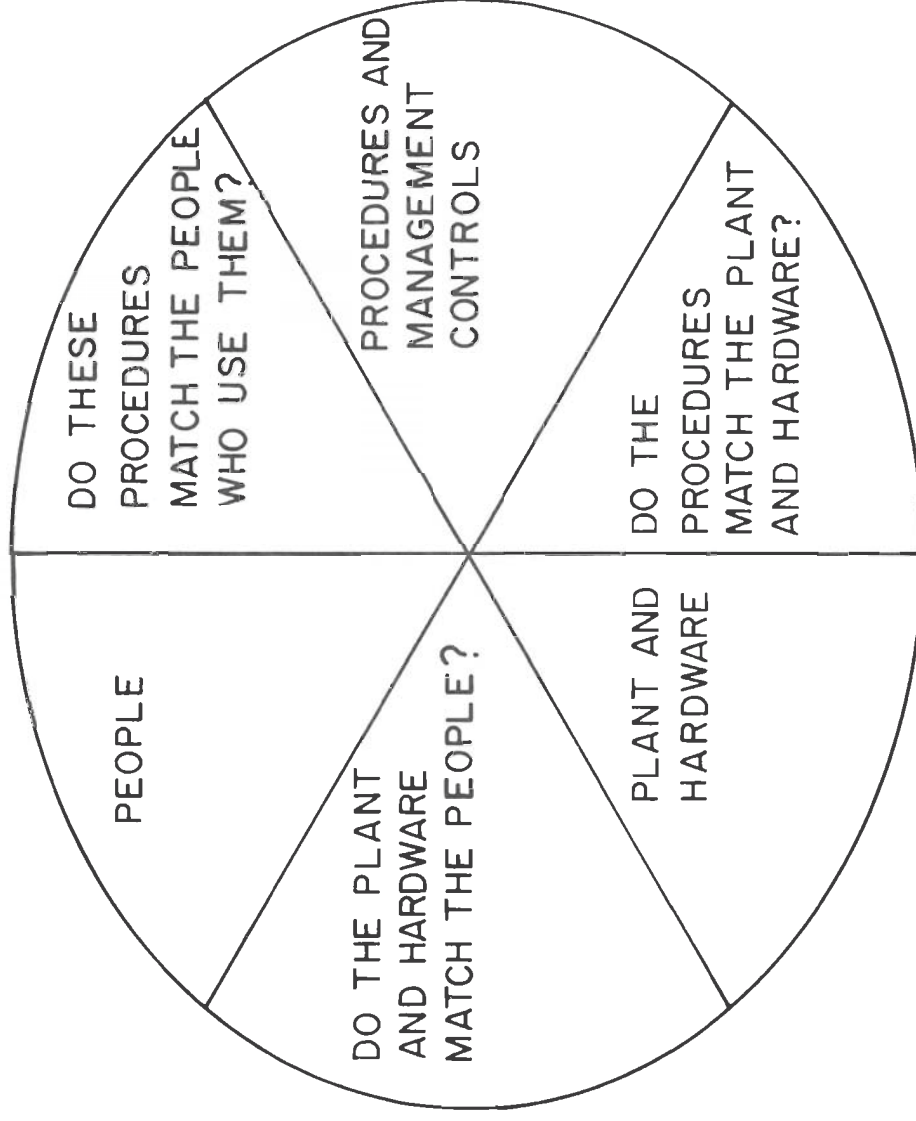


Fig. 1 Plant-people-procedures relationships.

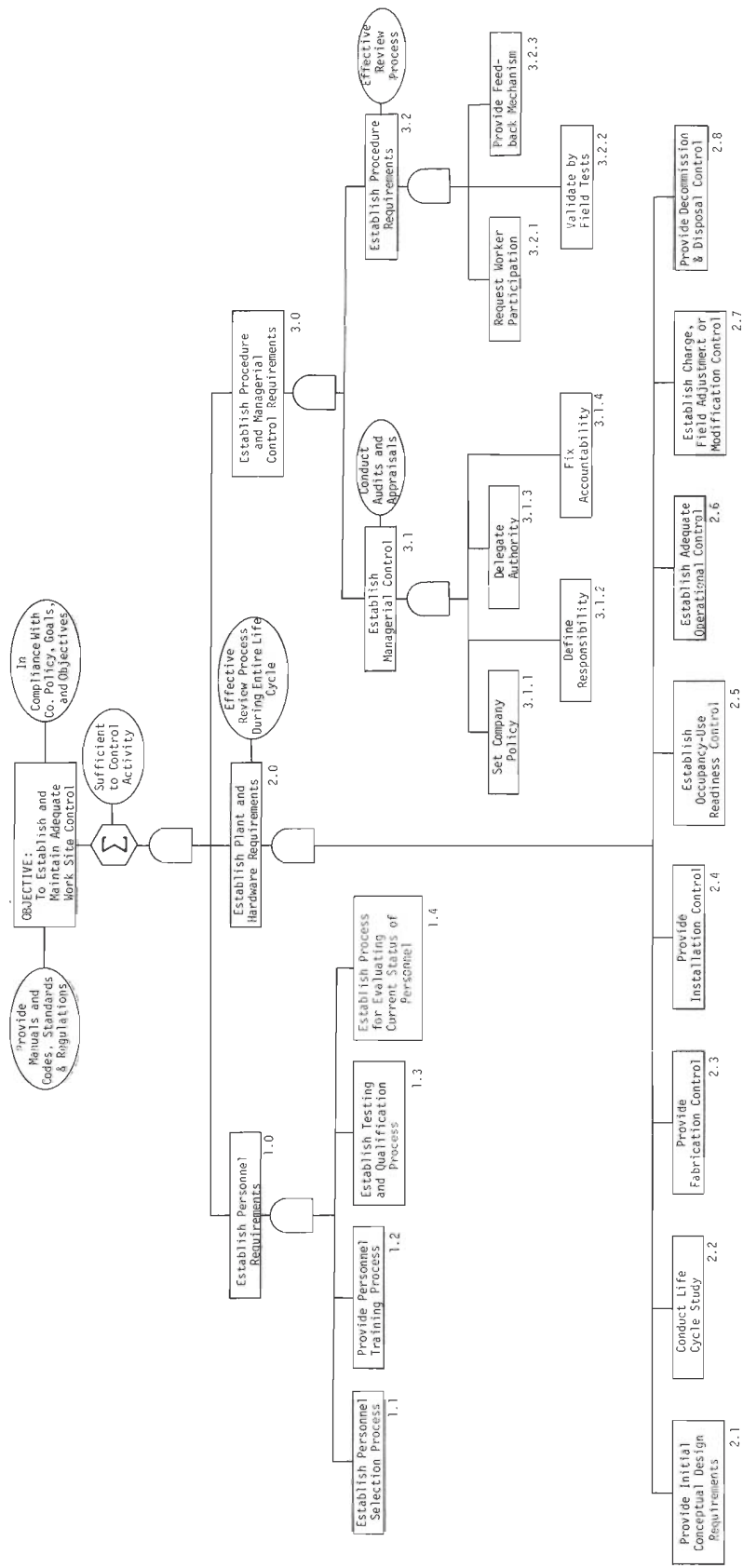


Fig. 2 The work process control tree.

The work process control tree (Figure 2) may help the user to identify problem areas in proposed or existing system. For some who are not familiar with decision trees, the work process schematic shown in Figure 3 is an alternate method for displaying the necessary elements needed to establish and maintain adequate worksite control. This schematic depicts how the "upstream processes" of personnel, hardware, and procedure begin to funnel down the necessary and sufficient elements, which assure that adequate worksite ingredients are produced. Shown on the right hand side of the schematic is the need of higher management to provide services to such people as supervising, scientific and engineering personnel, and working level personnel which will assist them in carrying out their responsibilities. The entire work process system is a highly complex network. The output of one work process subsystem (people, plant and hardware, and procedures) can serve as input into another. Therefore, it is necessary to evaluate each subsystem individually, and then the entire system as a whole.

If the analyst is not familiar with the process to be analyzed, he might find it difficult to (1) uncover discrepancies or deficiencies, (2) establish the most effective audit and review points, and (3) judge if a work process is ready to go here and now. One technique which has proven effective for the novice analyst is a simple flow charting method. This technique is outlined by the following steps:

- (1) Select a target system or subsystem.
- (2) Consider the entire life cycle of the system.
- (3) Read available documentation - interview "knowledgeable" and "responsible" people.
- (4) Break down the system into individual steps.
- (5) Flow chart the system.

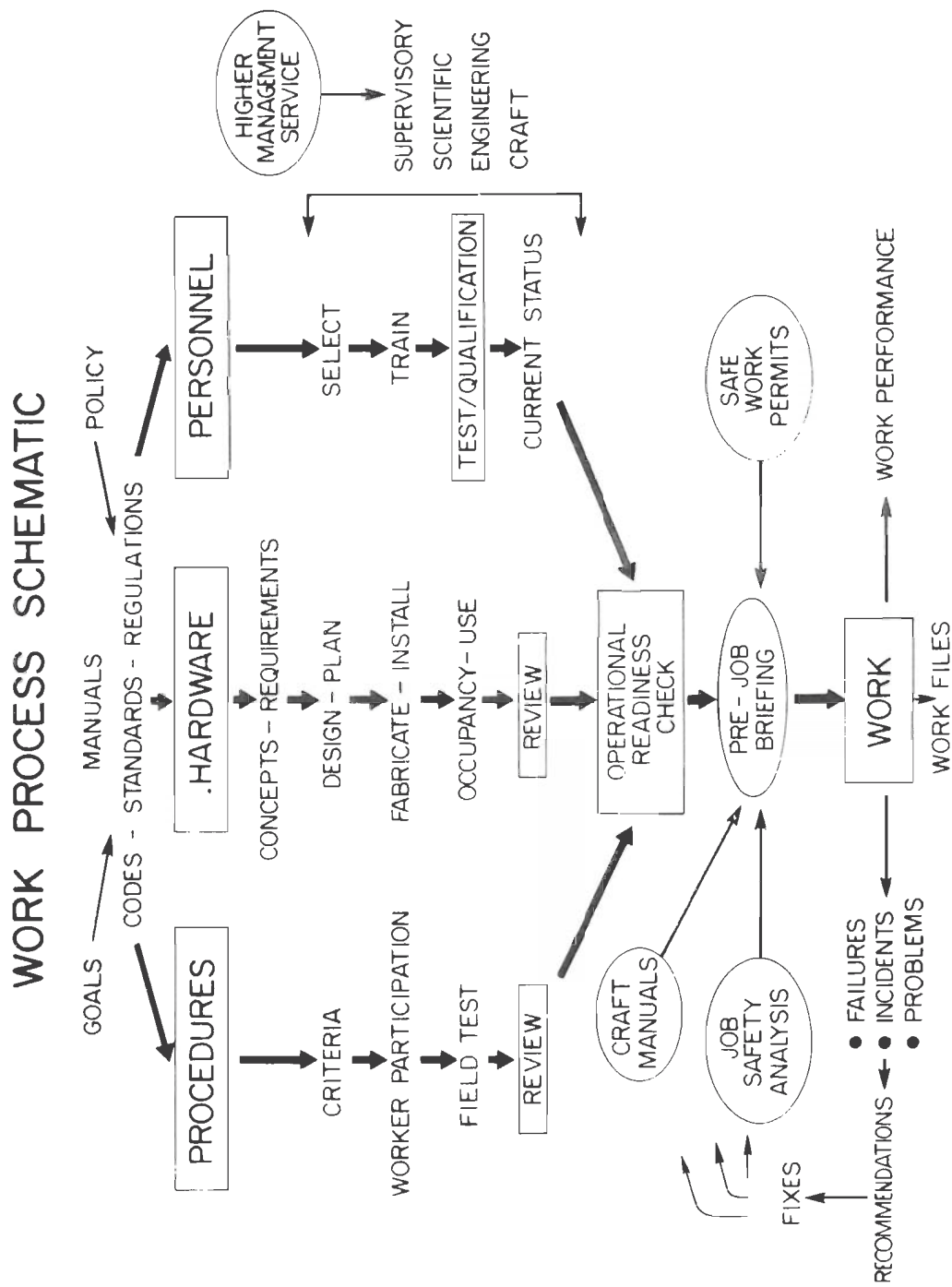


Fig. 3 The work process schematic.

- (6) Record pertinent observations and questions for each step.
- (7) Validate your flow chart with the appropriate personnel.
- (8) Take appropriate follow-up action.

An example of this flow charting method will be shown in a later section.

II. THE WORK PROCESS CONTROL TREE

To assist in the evaluation of existing or proposed worksite controls, criteria related to each element in the work process control tree (Figure 2) are listed below. The subsection numbering system below matches that of the tree and the criteria are proposed in question format. The questions should stimulate additional, more specific questions directly related to the work process in question.

To aid the novice in the use of the work process control tree (Figure 2), the following instructions are given:

- (1) The analyst is going to use Figure 2 to determine the adequacy of existing or proposed worksite control elements.
- (2) The elements in the tree can be broken down into more and more branches, as needed by the analyst.
- (3) These additional branches of the tree have been converted into a list of questions tabulated below.
- (4) It is suggested at this point that the analyst use the work process control tree with its associated question as a checklist to evaluate the system in question.

1.0 ESTABLISH PERSONNEL REQUIREMENTS

The "upstream processes" associated with the personnel part of the work process system would include such elements as establishing an employee selection process, providing adequate training, establishing a testing and qualification process, and evaluating the current status of each employee.

1.1 Establish Personnel Selection Process

Are criteria for selection defined?

Are the methods of personnel selection adequate to select individuals who meet the criteria established for the task?

Are the safety-related job requirements adequately defined to select an individual with desired characteristics?

Are personnel selected on the basis of the capability (both physical and mental) which is necessary and sufficient to perform the operation?

Is the help of appropriate professionals enlisted in the development of selection criteria?

Are employees selected by how well they match the environment in which they will be placed, as well as how well they will interface with the procedural and managerial controls? For example, are there adequate controls which will avoid placing tone-deaf or color blind individuals on critical control panels where tone and color perception are vital to correct performance?

1.2 Provide Personnel Training Process

Are there programs to adequately train personnel?

Is the individual trained for the task he or she is to perform?

Are the criteria used to establish the training program adequate in scope, depth, and detail?

Are the methods and personnel used in training adequate to meet training requirements?

Are personnel given the right amount of training for the equipment and procedures they will be using?

Are training programs within the company coordinated so that the employee gets the same messages from all the programs?

Does training adequately consider the employee's attitudes?

Is training updated to be current with changes in hardware, procedures, and management controls?

Is the training properly related to the written procedural material and direct supervisory attention provided?

Do all personnel have adequate knowledge regarding the risks they may accept personally and those which should be referred to higher management level?

Are foremen, supervisors, and managers trained in safety, risk management, identification of hazards, and risk acceptance?

1.3 Establish Testing and Qualification Process

Are testing and monitoring methods used to verify the adequacy of the training program (such as realistic simulators, tests and examinations)?

Is the verification of the person's current qualification status adequate?

Are testing and qualifying done on initial, continuous, and periodic bases?

Have assigned individuals been recently reexamined according to the criteria established for the task?

Are retraining and requalification requirements of the task defined and employed?

Are the professional skills of trainers measured and evaluated?

Is the training used at the worksite?

Do individuals demonstrate through "hands-on" use that they know how to apply the training properly?

Are there sufficient drills, exercises, and follow-up to provide proper reinforcement of training?

1.4 Establish Process for Evaluating Current Status of Personnel

Are supervisors' responsibilities defined? (Also staff support groups like personnel, medical, etc.?)

Do supervisors understand their responsibility in assessing the current status of their employees?

What aids are given supervisors in assessing the current status of their employees?

Are job performance indicators defined which might reveal personal problems?

Is there an employee assistance program to aid employees with problems such as drugs and alcohol?

Is there an ongoing medical program with periodic employee examinations?

Is there a structured supervisory observation plan in effect in the company?

Are there adequate controls in critical work processes on employees with personal problems?

Are medical personnel involved in accident/incident investigation and in feedback of relevant findings therefrom?

2.0 ESTABLISH PLANT AND HARDWARE REQUIREMENTS

If one were to closely examine any major hardware system, the need for auditing the upstream processes would be clearly demonstrated. The general hardware schematic, as shown in Figure 4, shows the major phases of a hardware life cycle, and is a prime example of how to use the flow charting technique discussed earlier. Also, the schematic reveals the necessity of review throughout the entire hardware lifetime. Review is especially important "early" in the cycle. By life cycle we mean the total womb-to-tomb sequence where one would give consideration to safety from the time that he once gets the gleam in his eye through design, fabrication, installation, operation, decommissioning, and disposal of the hardware. People have learned by sad experience that, had they given "early" consideration to the decommissioning and disposal of a piece of hardware, they probably would have designed it differently.

2.1 Provide Initial Conception and Design Requirements

In early design development, is the safety precedence sequence followed?

The safety precedence sequence is made up of the following key elements ranked in order of importance:

- (1) Design for Minimum Hazard. The major effort throughout the design phases should be to design for maximum inherent safety.

HARDWARE SCHEMATIC

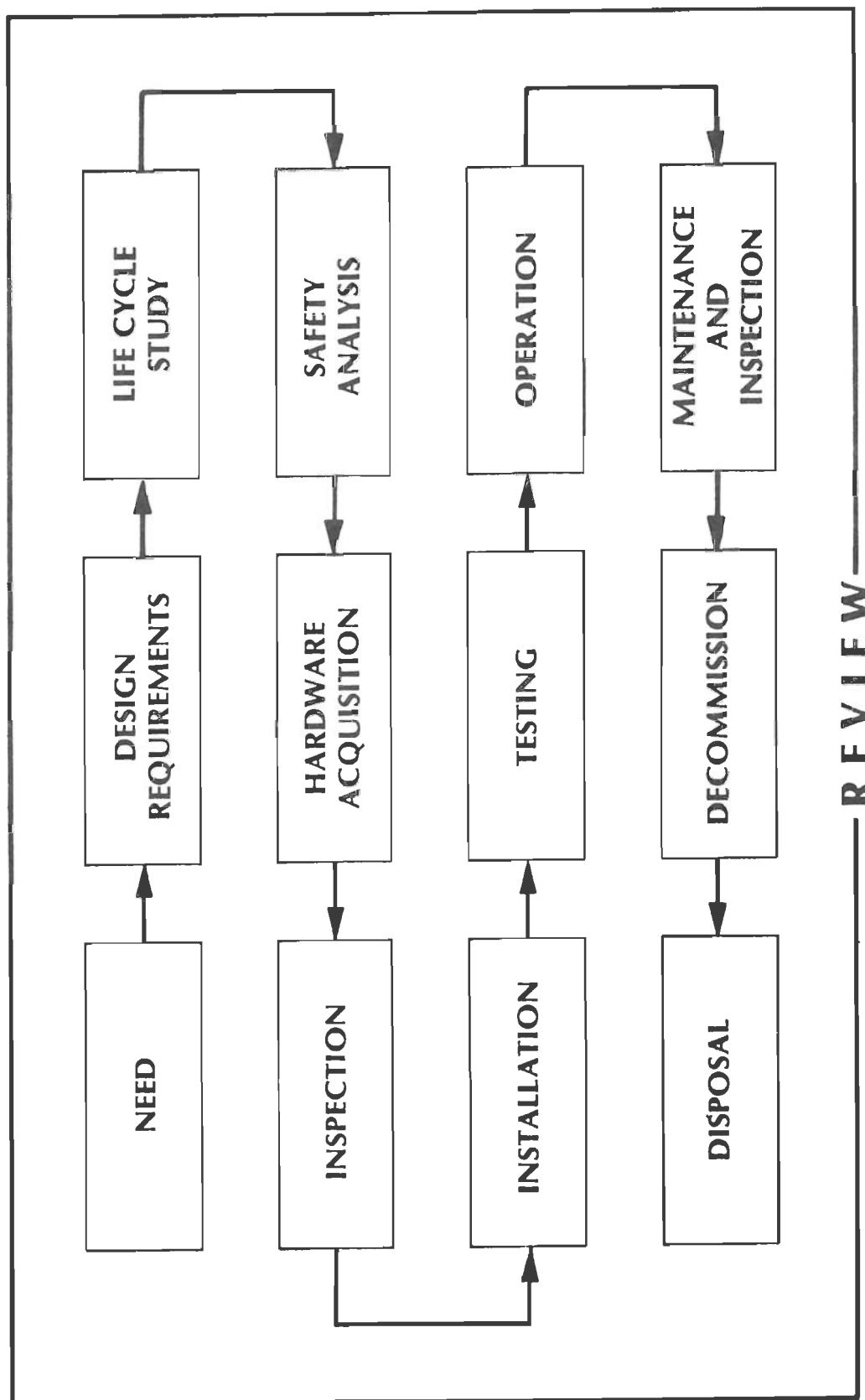


Fig. 4 The hardware schematic.

- (2) Reduce Hazards Through Safety Devices. Appropriate safety devices should be used in the system to reduce those hazards which cannot be controlled through design to an acceptable level.
- (3) Use Warning Devices to Warn of Hazards. Where hazards cannot be eliminated or reduced to acceptable levels, devices should be used that will detect hazardous conditions and provide a warning signal. (Also static warnings like "high voltage" signs, etc.)
- (4) Develop Procedures to Reduce Hazards. If the possible effects of an existing or potential hazard cannot be reduced through design or through safety and warning devices, special procedures must be developed for hazard control.
- (5) Identify the Residual Hazards. Any hazards remaining after application of the methods listed above must be communicated to management. Management must then decide whether or not the residual risks are acceptable.

Is the design a true representation of the developed criteria, definitions, specifications, and requirements?

Does the design of plant and equipment provide for safe shutdown and safety of persons and objects during all anticipated emergencies?

Are emergency procedures simple and easy to perform?

Has the design been reviewed against all applicable codes, standards, and regulations?

Is there an attempt, through design or procedures, to select less hazardous energy forms and to limit energy to that which is needed for the operation?

Has consideration been given in design, plan, and procedures to human characteristics as they compete and interface with machine and environmental characteristics?

Is there an attempt made to identify the ways and frequencies of human errors occurrence and thereby determine corrective action to reduce the overall error rate?

Is input from a human factors engineer requested and used in the engineering design phase?

Are controls selected which can be operated in short time with high reliability?

Are displays selected which can be interpreted in short time with high reliability?

Note: Appendix A contains additional reliability design review criteria which have been proven effective in developing adequate designs. The criteria are divided into three stages of design development: the conceptual review, the preliminary design review, and the final design review. Each phase contains questions which could be adapted for use as a checklist for safety review.

2.2 Conduct a Life Cycle Study

Is there an adequate safety analysis which starts with planning and continues through design, purchasing, fabrication, construction, operation, maintenance, and disposal?

Does the scope include not only the prime mission equipment, but also checkout and test equipment and procedures, facilities and operations, procedures for operation, selection of personnel, training equipment and procedures, maintenance facilities, equipment and procedures, and support equipment?

Is the life cycle analysis scoped to include an analysis of environmental impact which complies with all applicable requirements?

Is the requirement for life cycle analyses rigid enough to assure that analysis will be initiated during the planning stage?

Has sufficient consideration been given to special requirements, new problems, and other factors that are likely to be encountered if the facility/operation is modified or extended beyond its original intended life?

Is provision made for thorough and independent safety review at preestablished points (e.g., milestones) in the life cycle process?

2.3 Provide Fabrication Control

Are commonly recognized, good engineering practices, including safety, reliability, and quality assurance practices, adequately incorporated into the general fabrication process?

Are there written procedures which assure compliance with applicable engineering and design codes?

Where codes, standards, regulations, and state-of-the-art knowledge cannot furnish required fabrication data, are engineering studies conducted to obtain the needed information?

Is there an attempt to use proven, existing standardized parts and to design so as to encourage their use?

Are parts (particularly in-house fabricated parts) clearly identified and marked?

Are fabrication controls placed on both in-house and out-of-house work?

Is the safety/quality interface well-defined so that safety-related specifications and criteria identified in the safety analysis and review are considered in defining quality assurance criteria?

Are quality assurance and inspection criteria defined?

Are there adequate controls on as-built documentation?

Are specifications, analyses, and other software updated to match "as-fabricated" hardware?

2.4 Provide Installation Control

Is hardware protected to prevent degradation of quality and safety between fabrication and installation?

Does the installation description provide the clear and concise information needed by installation personnel?

Is an adequate reliability and quality assurance program integrated into the installation process?

Is the actual physical arrangement or configuration identical with that required by latest drawings, specifications, and procedures?

2.5 Establish Occupancy-Use Readiness Control

Is verification of the facility and/or work process adequate? (A publication of the System Safety Development Center, SSDC-1^[3] provides detailed criteria for this major functional branch.)

Are acceptance criteria stringent enough to assure operability/maintainability and compliance with final design?

Is there adequate testing during development of a new design to demonstrate that it will serve its intended function?

Does qualification testing assure that nonstandard components satisfy the acceptance criteria?

Is the performance of an operational readiness review specified?

Is the occupancy-use readiness process and criteria adequate to assure functional operability?

Is an acceptable procedure for determining occupancy-use readiness prepared and followed?

Are the personnel who made the decision on occupancy-use readiness adequately skilled and experienced?

Is the follow-up of action items from occupancy-use readiness review adequate? Are all outstanding action items resolved prior to startup of the work flow process?

2.6 Establish Adequate Operational Control

Are there adequate operational specifications for all phases of the system operation?

Is there a "dry run" or demonstration to prove out all associated hardware and procedures, check for oversights, adjust for the final arrangement, and provide for first "hands-on" participation?

Have all applicable and appropriate safety requirements been specified, made available, and used?

Is all applicable documentation complete, up-to-date, and accessible to users?

Are obsolete documentation and hardware removed from the system?

Is the work force given a pretask briefing (prior to task performance)? Is it adequate? Does the pretask briefing adequately consider the net effect of recent changes, maintenance, new hazards, etc.?

Is there adequate technical support furnished to the worksite? Are the organizational and functional requirements adequate to assure the required level of operability?

Is the interface between operations personnel and testing and maintenance personnel adequate? Are administrative procedures well-planned to preclude misunderstanding of operational status due to a breakdown of communications?

Is an analysis performed for each work task involving a high potential for error, injury, damage, or for encountering an unwanted energy flow?

Is the hazard identification and analysis process properly conceptualized, defined, and executed?

Is task safety analysis performed as part of the work process [such as the Job Safety Analysis (JSA)^[4] which is summarized in Figure 5]?

Have the necessary criteria been specified and elements defined to adequately support the safety analysis program?

Are there adequate maintenance and inspection of equipment, processes, utilities, operations, etc.?

Are the maintenance and inspection plans broad enough to include all the areas that should be maintained and inspected? Is management aware of those areas not included in the plan?

SUMMARY OF JOB SAFETY ANALYSIS (EMPLOYEE PARTICIPATION PROGRAM)

- GOAL (1) DETERMINE POTENTIAL ACCIDENT CAUSES.
(2) ELIMINATE POTENTIAL ACCIDENT CAUSES.
- I. DETERMINE JOBS TO BE ANALYZED.
 - II. ESTABLISH PRIORITY IN WHICH JOBS ARE TO BE ANALYZED.
 - A. FREQUENCY (OF ASSOCIATED ACCIDENTS)
 - B. SEVERITY (ACCIDENT POTENTIAL)
 - C. SUPERVISORY JUDGMENT
 - D. REGULARITY (HIGH EXPOSURE RATE)
 - E. JOB CHANGES (HAZARDS NOT CLEAR)

} FIVE STEPS TO
DECIDE PROPER
PRIORITY
 - III. METHOD
 - A. GROUP DISCUSSION METHOD
 - B. DIRECT OBSERVATION METHOD
 - IV. BREAK DOWN INDIVIDUAL JOB INTO STEPS OR ELEMENTS.
 - V. DETERMINE THE CONTACT POSSIBILITIES (ENVIRONMENT)
 - A. CAN THE WORKMAN BE STRUCK BY ANYTHING WHILE DOING THE JOB STEP?

 NOTE: AT THIS POINT - UNLESS TIME PROHIBITS - DO NOT CONSIDER WAYS OF PREVENTING CONTACT - ONLY IDENTIFY THE CONTACT POSSIBILITIES?
 - B. CAN THE WORKMAN STRIKE AGAINST ANYTHING DOING THE JOB STEP? (IT IS IMPORTANT, NOT ONLY TO IDENTIFY WHAT THE WORKMAN CAN STRIKE AGAINST, BUT ALSO HOW THE CONTACT COULD COME ABOUT.)
 - C. CAN THE WORKMAN BE CAUGHT BETWEEN ANY OBJECTS DOING THE JOB STEP? (e.g., LOOK FOR "PINCH" POINTS).
 - D. CAN THE WORKMAN BE CAUGHT ON OR IN ANYTHING DOING THE JOB STEP? (e.g., CLOTHING IN MACHINERY).
 - E. CAN THE WORKMAN FALL DOING THE JOB STEP?
 - F. MISCELLANEOUS ACCIDENT POSSIBILITIES.
 - VI. ELIMINATE OR REDUCE CONTACT POSSIBILITIES.
 - A. ESTABLISH A SAFE WORK PROCEDURE THAT WILL ELIMINATE OR REDUCE THE POTENTIAL CONTACTS.
 - B. CHANGE THE CONDITION OF THE ENVIRONMENT WHICH CONTRIBUTES TO THE POSSIBILITY OF A CONTACT (TOOLS, EQUIPMENT, MACHINES, etc.).
 - C. WEARING PERSONAL PROTECTIVE APPAREL
 - VII. DEVELOP SAFE PROCEDURE
 - VIII. SAFE JOB PROCEDURE APPRAISAL
 - A. ON-THE-JOB REVIEW
 - B. CONFERENCE REVIEW
 - C. MANAGEMENT REVIEW

} EMPLOYEE
PARTICIPATION

Fig. 5 The summary of job safety analysis.

Do the plans require that failed items be analyzed for cause of failure? Are the analysis results required to be acted upon by an appropriate individual or group?

Are maintainability and inspectability requirements specified by the design or procurement documents? If not, are they provided adequately by operations plans?

Do the plans address methods for minimizing problems with equipment, processes, utilities, operations, etc., when they are undergoing maintenance or inspection?

Are there logs or other evidence of maintenance and inspections kept at the point-of-operation of equipment, process, etc.?

2.7 Establish Change, Field Adjustment, or Modification Control

Has a specific change-based analytic method been established to review form, fit, or function of components and subsystems?

Is there a formal program to assure adequate configuration control throughout the entire life cycle of the facility? Does the program allow for review of modified procedures, drawings, and other documentation?

Are the hardware configuration and documentation of a modification to the facility or process adequately controlled?

Are the triggers (stimuli) for the initiation of the Hazard Analysis Process (HAP) adequate? Are they utilized to obtain early safety participation and review in planned or unplanned changes?

What guidance is given to supervisors on review methods and change detection?

Are counterchanges made for the known changes when appropriate?

Do all personnel have adequate knowledge regarding the risks they may accept personally and those which should be referred to higher management level?

2.8 Provide Decommission and Disposal Control

Is the design such that disposal problems and hazards are minimized when the facility or operation has served its useful life?

Is consideration given to the effects decommissioning and disposal will have upon the environment? During operation? At the conclusion of operation?

If hardware will have to be dismantled for disposal, is consideration given to design the hardware in modular sections?

3.0 ESTABLISH PROCEDURAL AND MANAGERIAL CONTROL REQUIREMENTS

The third major element in the work process system is the development of procedures and the implementation of managerial controls.

3.1 Establish Managerial Control

Is there a written, up-to-date policy with a broad enough scope to address major problems likely to be encountered? Is it also sufficiently comprehensive to include the major concerns (e.g., humane, cost, efficiency, legal compliance)? Can it be implemented without conflict?

Does the overall program fulfill the intention of the policy statement? If there are problems encountered in implementing the policy, are these relayed back to the policy makers? Is the implementation a continuous, balanced effort designed to correct systemic failures, and generally predictive rather than reactive?

Is safety policy implemented by directives which emphasize methods and functions of hazard review, monitoring, etc., in addition to specific rules for kinds of hazards? Are directives published in a style conducive to understanding and without interface gaps?

Has management provided the type of supportive services and guidance needed at the lower organization levels? Is there a formal development program for all management personnel which addresses: (1) general aspects of management and supervision, (2) specific technologies, (3) human relations/communications, and (4) safety?

Are definitive criteria provided which assure risk acceptance only at proper management levels?

Is line management held accountable for safety functions under their jurisdiction? If so, are there methods for measuring their performance?

Have top management individuals demonstrated an interest in lower level program activities through personal involvement? Is their concern known, respected, and reflected at all management and employee levels?

Are there guidelines and rules for supervisory needs, capabilities, and responsibilities?

Are the help and assistance given to supervisors adequate to enable them to fulfill their roles? Is the feedback of information to the supervisor adequate? Is it furnished in a form usable by the supervisor? What training has the supervisor been given in general supervision? What training has the supervisor been given in safety? Has a supervisor training program been evaluated?

3.2 Establish Procedural Requirements

Do the procedures for each task meet selection and training criteria and the applicable operating criteria? Are the procedures responsive to supervisory problems?

Do engineers and designers recognize their limitations in writing procedures for operating personnel, and of the need for selection and training criteria for operators, and of supervisory problems?

Are there sufficient checkpoints in written procedures to assure that steps are being done correctly?

Are procedures revised, as necessary, to agree with changes in plant or equipment?

Does the writing style of the procedures give consideration to variations in reading skills and intelligence of intended users? Are procedures sufficiently scoped and detailed to adequately cover all steps of a task?

Are procedures validated with applicable criteria and tested for correctness under "dry run" operating conditions?

Do procedures give users clear instructions for all anticipated emergency conditions? Are instructions easy to follow under the stress of an emergency?

Are dynamic and static warnings used when appropriate? Are they located at point-of-operation as well as in procedures? Is their meaning unambiguous?

Are procedures written in such a way as to assure that the step is in an order of logic sequence?

Are lockouts and procedures used where hazardous situations are encountered or created?

Do the procedures adequately convey their intended message? If procedures call for coordination between users and other individuals, are these interfaces clear?

Is the process of accomplishing the JSA program adequately defined and staffed? Is work level employee participation requested in preparing JSAs?

Is consideration of employee-developed suggestions and inputs adequate?

Is information on deficient procedures fed back to the procedure writers and responsible management?

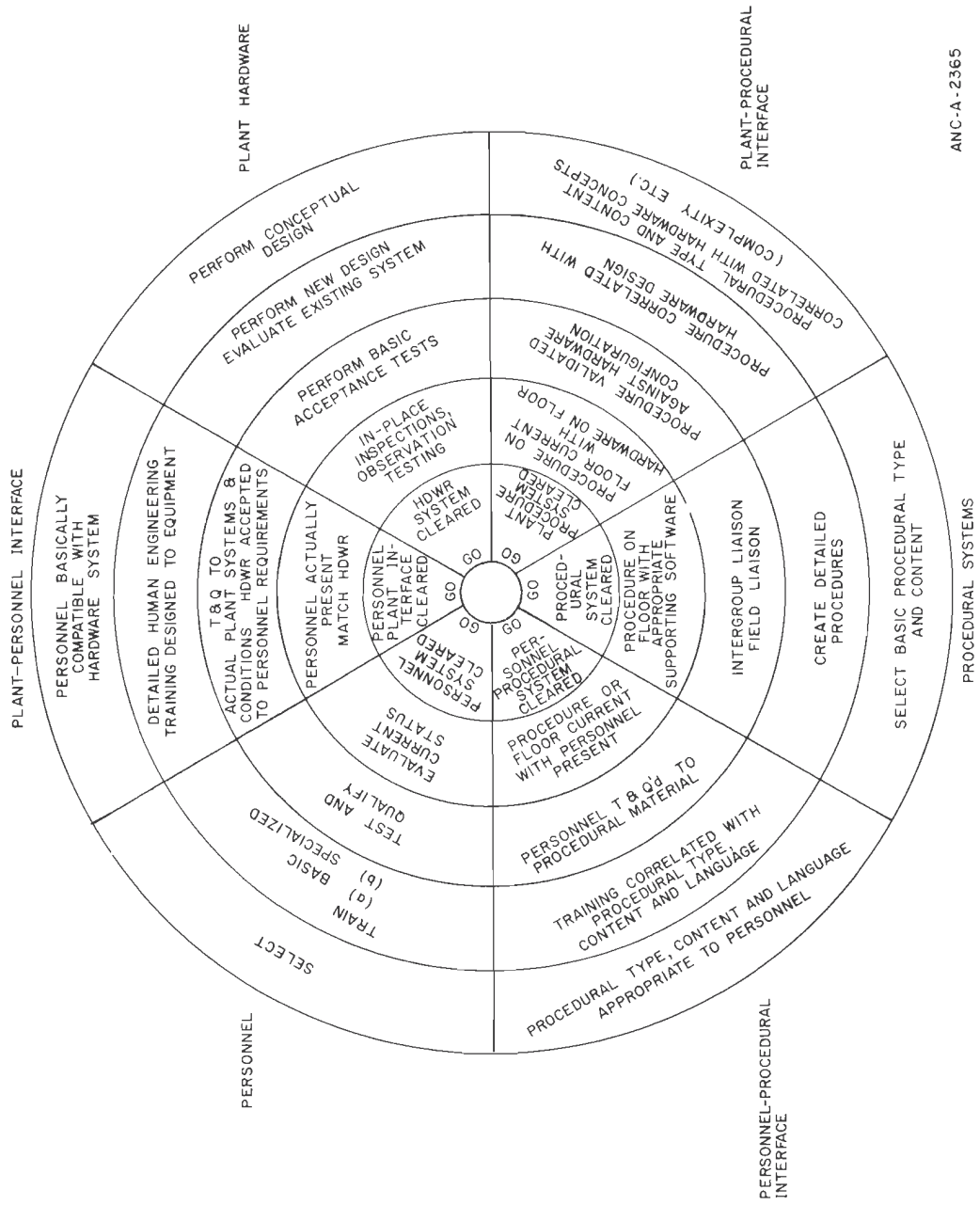
Note: Appendix B contains detailed criteria for the preparation or review of procedures. The criteria are arranged in such a way that they can be used as a checklist.

III. CONCLUSION

In this Guide, have been discussed some of the upstream processes which produce the worksite ingredients. The people-plant-procedure relationships and the required managerial controls were indicated.

Also methods were given to aid the user in the evaluation of existing or proposed system. These methods should aid the user in identifying discrepancies and deficiencies.

Once we have analyzed the system and determined our weaknesses, we then can begin to add our controls on the processes which produce the worksite ingredients. Figure 6^[5] shows the application of these controls through a portion of the life cycle system leading to the actual performance at the worksite. This Figure is derived from Figure 1, logically, Figure 1 is a one-dimensional (\emptyset) plot. Figure 6 is a corresponding two-dimensional display, (\emptyset , R) where the distance from the origin is a measure of the time from start-up. This Figure begins to show the various interrelationships between the people, plant, and procedures in a time dependent sequence from conception to the actual job of work being performed. Figure 6 can be used as an occupancy-use readiness, checklist prior to new or modified system start-up, or even at the beginning of a new day on existing systems. With the implementation of these types of controls, adequate worksite control is beginning to be established and maintained.



ANC-A-2365

Fig. 6 The application of system controls.

IV. REFERENCES

- [1] W. C. Pope, et al., Safety Aids Decision Making, National Safety Management Society.
- [2] W. G. Johnson, MORT - The Management Oversight and Risk Tree, SAN 821-2 (February 1973).
- [3] R. J. Nertney, J. L. Clark, and R. W. Eicher, Occupancy-Use Readiness Manual - Safety Considerations, ERDA-76-45-1, SSDC-1 (September 1975).
- [4] Principles of Accident Prevention, U. S. Steel Corporation (1968).
- [5] R. J. Nertney and M. G. Bullock, Human Factors in Design, ERDA-76-2, SSDC-2 (February 1976).

APPENDIX A

DESIGN REVIEW CRITERIA

A. Conceptual Review

1. Have the operational performance criteria been established and documented?
2. Have the operational environmental criteria been established and documented?
3. Do the established performance and environmental criteria meet customer requirements?
4. Have the operational safety and reliability requirements been established?
5. Does the predicted reliability meet the reliability requirements?
6. Have alternate designs been investigated and an optimum selection made?

B. Preliminary Design Review

1. Have the checklist items for the conceptual review been answered satisfactorily?
2. Has a failure modes and effects analysis been completed?
3. Have all preventive/corrective actions been initiated to eliminate or minimize all modes of failure?
4. Does the current reliability assessment and prediction indicate that the reliability requirements will be met?
5. Have safety and reliability analyses been made for alternate designs?

6. Have trade-off relationships of reliability vs. such criteria as weight, volume, maintainability, cost, schedule, and producibility been maximized?
7. Are safety margins for the design adequate to compensate for uncertainties in material properties, loads, environments, and analytical methods?
8. Do the design specification performance limits represent values which can be attained within the development program?
9. Will the development test program as planned evaluate the performance capability of the assembly or component in all critical modes of operation to be met in qualification testing?
10. Will development tests permit evaluation of critical modes-of-failure and the ability of the assembly or component to meet specified performance limits?
11. Has a test program which includes peripheral testing been planned to investigate the achievement of specific characteristics and pertinent modes of failure?
12. Have all doubtful areas of material applications in the assembly or component relative to fatigue, creep, corrosion, etc., been investigated by the Materials Engineering Division?
13. Has a final stress analysis of the assembly or component been completed?
14. Has a complete dynamic analysis been accomplished?
15. Does the assembly or component design provide for efficiency in inspection and replaceability for restoration to operational effectiveness?

16. Will manufacturing and inspection variability in dimensions and processing degrade reliability below an acceptable level?
17. Have process control procedures and inspection procedures been prepared for all assembly or component fabrication operations requiring high accuracy of adjustment, special equipment, special tools, and techniques; or where inaccessibility creates special problems?
18. Does the design incorporate positive features that prohibit incorrect installations?
19. Have adequate protective equipment and procedures been provided to prevent damage to the assembly or component during fabrication handling, testing, cleaning, and shipping to prevent degradation of reliability?
20. Is the design conducive to the maintenance of cleanliness and corrosion resistance?
21. Have all items requiring identification and traceability been identified?
22. Have all reliability sensitive components been identified?
23. Has a parts application review been conducted for all purchased parts?
24. Have all safety criteria and specifications been included?

C. Final Design Review

1. Have the checklist items for the preliminary design review been answered satisfactorily?

2. Do the design specifications conform to customer requirements?
3. Have the drawings met all checking requirements?
4. Are the process and material specifications released?
5. Do the design specifications, drawings, and process and material specifications contain all necessary reliability assurance provisions?
6. Does the current reliability assessment and prediction indicate that the reliability requirements will be met?
7. Has a reliability demonstration plan been established?
8. Have all action items from previous reviews been completed?
9. Have all safety and reliability problems been resolved?
10. Has an integrated test program been defined including incorporation of statistical techniques and reliability testing provisions?
11. If the design contains subcontractor or vendor supplied parts, have subcontractor and vendor reliability assurance provisions been required?

APPENDIX B

CRITERIA FOR PREPARATION OR REVIEW OF PROCEDURES

A. Correlation Between Procedure and Hardware

1. Does the procedure contain a statement as to the hardware configuration for which it is written?
2. Does the procedure contain background descriptive or explanatory information where needed?
3. Does the procedure reflect or reference the latest revision to drawings, manuals, or other procedures?

B. Adequacy of the Procedure

1. Is this the best way to do the job?
2. Is the procedure clear, concise, and free from ambiguity which could lead to wrong decisions or actions?
3. Have calibration requirements been clearly defined?
4. Have critical red-line parameters been identified and clearly defined, and have required values been specified?
5. Have corrective controls of these parameters been clearly defined?
6. Are all values, switches, and other controlling components identified and defined?
7. Are such items as pressure limits, caution notes, safety distances, or hazards peculiar to this operation clearly defined?
8. Is the procedure easy to understand?

9. Are hard-to-locate components adequately described and located?
10. Are job safety requirements defined, e.g., power off, pressure down, and tools checked for sufficiency?
11. Is system operative at end of job (system status)?
12. Is detail appropriate - not too much, not too little?
13. Has the hardware involved in the procedure been evaluated for human factors and behavioral stereotype problems? (If not corrected, are any such clearly identified?)
14. Are monitoring points and methods of verifying adherence specified?
15. Is maintenance and/or inspection to be verified? If so, is a log provided?
16. Is safe placement of other process personnel or of equipment specified?
17. Were errors in previous, similar processes studied for cause? Does this procedure correct such causes?
18. Have jigs and arrangements been provided to minimize error?

C. Accuracy of the Procedure

1. Has the capacity of this procedure to accomplish its specified purpose been verified by internal review?
2. Are all gauges, controls, valves, etc., which are called out in this procedure, described exactly as they are labeled?

3. Are all setpoints or other critical controls, etc., compatible with values given in control documents and stated in the procedure?
4. Are the safety limitations in this procedure adequate for the job to be performed?
5. Are all steps in the proper sequence?

D. References to Supporting Documentation

1. Are all supporting drawings, manuals, data sheets, sketches, etc., either listed in this procedure or attached?
2. Are all interfacing procedures listed in this procedure?

E. Securing Provisions

1. Does the procedure contain adequate instructions to return the facility or hardware to a safe operating or standby condition?
2. Do these securing instructions contain step-by-step operations?

F. Backout Provisions

1. Can this procedure put any component or system in a condition which could be dangerous?
2. If so, does this procedure contain emergency shutdown or backout procedures either in an appendix to the procedure or as an integral part of the procedure?
3. Is the backout procedure or instructions for its use included at the proper place in the basic procedure?

G. Emergency Measures

1. Are there procedures for action in case of emergency conditions?
2. Does the procedure involve critical actions such that preperformance briefing on possible hazards is required?
3. Are adequate instructions either included or available for action to be taken under emergency conditions? Are they in the right place?
4. Are adequate shutdown procedures available and do they cover all systems involved, and are they available for emergency reentry teams?
5. Does the procedure specify the requirements for an emergency team for accident recovery, troubleshooting, or investigative purposes where necessary, and describe the conditions under which the emergency team will be used and the hazards they may encounter or must avoid?
6. Does the procedure consider interfaces in shutdown procedures?
7. How will changes be handled? What are thresholds for changes requiring review?
8. Have emergency procedures been tested under the range of conditions which may be encountered, e.g., at night during power failure?

H. Caution and Warning Notes

1. Have caution and warning notes been included where appropriate?

2. Do caution and warning notes precede the operational steps containing potential hazards?
3. Are they adequate to describe the potential hazard?
4. Are they separate entries with distinctive bold type or other emphatic display?
5. Do they include supporting safety control (health physics, safety engineer, etc.) if needed at specific required steps in the procedure?
6. Are human-induced hazards identified and described by cautions and warnings?

I. Requirements for Communications and Instrumentation

1. Has an adequate means of communication been provided?
2. Will loss of communications create a hazard?
3. Is the course of action clearly defined in the event of loss of required communications?
4. Has verification of critical communication been included where required?
5. Will loss of control or monitoring capability of critical functions create a hazard to people or hardware?
6. Have alternate means or a course of action been clearly defined to regain control of monitoring functions?
7. Are the above situations flagged by cautions and warnings?

J. Sequence-of-Events Considerations

1. Can any operation in the procedure initiate an unscheduled or out-of-sequence event?
2. Could it induce a hazardous condition?
3. Is it identified by warnings or cautions?
4. Is it covered by emergency shutdown and backout procedures?
5. Are all sequence steps prescribed in the procedure sequence properly and such that they will not contribute to or create a hazard to the hardware?
6. Have all steps been identified and flagged which could cause a hazard if performed out-of-sequence?
7. Have all noncompatible simultaneous operations been identified and suitably restricted?
8. Have these been prohibited by positive callout or separation in step-by-step inclusion within the text of the procedure?

K. Environmental Considerations (Natural or Induced)

1. Have environmental requirements been specified which contain the initiative of the procedure or which would require shut-down of the action or evacuation, once in progress?
2. Have the induced environments (radioactive, toxic, or explosive atmospheres, etc.) been considered?
3. Have all latent hazards (pressure, height, voltage, etc.) in adjacent environments been considered?

4. Are there induced hazards from simultaneous performance of more than one procedure by personnel within a given area?

L. Personnel Qualification Statements

1. Has a requirement for certified personnel been considered?
2. Is required frequency of requalification of personnel specified?

M. Interfacing Hardware and Procedures Noted

1. Have all interfaces been described by detailed callout?
2. Have interfacing operating procedures been identified or written to ready equipment?
3. Where more than one organizational element is involved in an operation, have proper liaison and areas of responsibility been established?

N. Procedure Sign-off

1. Is procedure to be used as an in-hand, literal checklist?
2. Have step-by-step sign-off requirements been considered and identified and appropriate spaces in the procedure provided?
3. Have procedure completion sign-off requirements been indicated (signature, authority, date, etc.)?
4. Is supervisor verification of correct performance required?

0. General Requirements

1. Are the procedures set up such as to discourage a shift change during performance or in such a manner as to accommodate a shift change?
2. Where shift changes are necessary, does the procedure include or reference shift overlap and briefing requirements?
3. Is there mandatory inspection, verification, and system validation required whenever the procedure requires breaking into and reconnecting a system?
4. Are safety prerequisites defined? Have all safety instructions been spelled out in detail to all personnel?
5. Do the procedures require prechecks of supporting equipment to ensure its compatibility and availability?
6. Has consideration for unique operations been written into the procedures?
7. Do the procedures require walk-through or talk-through dry runs?
8. General supervision requirements, e.g., what is the protocol for transfer of supervisor responsibilities to a successor?
9. Are the responsibilities of higher supervision specified?

P. Reference Considerations

1. Have applicable quality assurance and reliability standards been considered?

2. Have applicable codes, standards, and regulations been considered?
3. Does the procedure comply with control documents?
4. Have hazards and system safety degradations been identified and considered against specific control standards and procedures?
5. Have specific prerequisite administrative and other management approvals been complied with?
6. Have comments been received from the people who will do the work?

Q. Special Considerations

1. Has a documented safety analysis been considered for safety-related deviations from normal practices or for unusual or unpracticed maneuvers?
2. Have new restrictions or controls become effective that affect the procedure in such a manner that new safety analyses may be required?

OTHER SSDC PUBLICATIONS IN THIS SERIES

SSDC-1	Occupancy-Use Readiness Manual
SSDC-2	Human Factors in Design
SSDC-3	A Contractor Guide to Advance Preparation for Accident Investigation
SSDC-4	MORT User's Manual
SSDC-5	Reported Significant Observation (RSO) Studies
SSDC-6	Training as Related to Behavioral Change
SSDC-7B	DOE Guide to the Classification of Recordable Accidents
SSDC-8	Standardization Guide for Construction and Use of MORT-Type Analytic Trees
SSDC-9	Safety Information System Guide
SSDC-10	Safety Information System Cataloging
SSDC-11	Risk Management Guide
SSDC-12	Safety Considerations in Evaluation of Maintenance Programs
SSDC-13	Management Factors in Accident/Incidents (Including Management Self-Evaluation Checksheets)
SSDC-14	Events and Causal Factors Charting
SSDC-15	Work Process Control Guide
SSDC-16	SPRO Drilling and Completion Operations
SSDC-17	Applications of MORT to Review of Safety Analyses
SSDC-18	Safety Performance Measurement System
SSDC-19	Job Safety Analysis
SSDC-20	Management Evaluation and Control of Release of Hazardous Materials

OTHER SSDC PUBLICATIONS (Continued)

SSDC-21	Change Control and Analysis
SSDC-22	Reliability and Fault Tree Analysis Guide
SSDC-23	Safety Appraisal Guide
SSDC-24	Safety Assurance System Summary (SASS) Manual for Appraisal
SSDC-25	Effective Safety Review
SSDC-26	Construction Safety Monographs (a series of 18)
SSDC-27	Accident/Incident Investigation Manual (Second Edition)
SSDC-28	Glossary of SSDC Terms and Acronyms
SSDC-29	Barrier Analysis
SSDC-30	Human Factors Management
SSDC-31	The Process of Task Analysis
SSDC-32	The Impact of the Human on System Safety Analysis
SSDC-33	The MORT Program and the Safety Performance Measurement System
SSDC-34	Basic Human Factors Considerations
SSDC-35	A Guide for the Evaluation of Displays
SSDC-36	MORT-Based Safety Professional/Program Development and Improvement
SSDC-37	Time/Loss Analysis
SSDC-38	Safety Considerations for Security Programs
SSDC-39	Process Operational Readiness and Operational Readiness Follow-on