

**NASA TECHNICAL  
MEMORANDUM**

NASA TM X-71697

NASA TM X-71697

(NASA-TM-X-71697) SAFETY MANAGEMENT OF A  
COMPLEX R AND D GROUND OPERATING SYSTEM  
(NASA) CSCL 05A

N75-22183

Unclas  
G3/81 18649

**PRICES SUBJECT TO CHANGE**

**SAFETY MANAGEMENT OF A COMPLEX R & D  
GROUND OPERATING SYSTEM**

by James F. Connors and Roy A. Maurer  
Lewis Research Center  
Cleveland, Ohio 44135

TECHNICAL PAPER presented at  
Annual Safety Symposium on the Engineering  
Aspects of Safety sponsored by Federal Occupational  
Safety and Health Council of Southern California  
Port Hueneme, California, February 20, 1975

Reproduced by  
**NATIONAL TECHNICAL  
INFORMATION SERVICE**  
US Department of Commerce  
Springfield, VA. 22151

SAFETY MANAGEMENT OF A COMPLEX R&D  
GROUND OPERATING SYSTEM

James F. Connors\* and Roy A. Maurer†

Lewis Research Center

SUMMARY

A perspective on safety program management has been developed for a complex R&D operating system, such as the NASA-Lewis Research Center. Using a systems approach, hazardous operations are subjected to third-party reviews by designated area safety committees and are maintained under safety permit controls. To insure personnel alertness, emergency containment forces and employees are trained in dry-run emergency simulation exercises. The keys to real safety effectiveness are top management support and visibility of residual risks.

INTRODUCTION

Generally, everyone subscribes to the basic concept of safety; i.e., the protection of life and limb of personnel, the protection of facilities and equipment, and the minimization of disruption to operations. However, there also seems to be a certain amount of semantics and disparity involved in how the various agencies pursue, organize and manage against these noble objectives. Functionally, safety is all pervasive! In the technology business, it encompasses virtually all of the technical disciplines. To insure system effectiveness, safety surveillance of hazardous activities must extend from womb to tomb, or from concept through operations.

[Note: References 1 through 9 provide the literature backdrops against which the viewpoints and safety philosophies expressed herein are made. Basically, the approach is from the perspective of safety program managers rather than "experts" in safety.]

What then is the so-called "safety man" or the safety engineer? Certainly, there is no single omniscient individual versed in all technical disciplines that can provide all the safety solutions. In working with complex systems, we must bring to bear

---

\*Director of Technical Services

†Chief, Safety and Project Planning Office

the best expert knowledge available to us and appropriate to the issues before us. For example, today when dealing with high pressure systems, we must necessarily involve one versed in fracture mechanics and fracture control---one whose analyses and judgments we can rely on. With the systems approach, the safety officer's job is more one of operations review, coordination, management and implementation of procedures. In the assurance of safety, he must achieve continuity of surveillance throughout the life cycle of the activity. Subdividing safety into system safety, aviation safety, industrial safety, public safety, etc., doesn't appear to make much sense and only achieves jurisdictional gaps and overlaps. The safety man's goal is to insure that the right questions are asked: Have all the hazards been identified? Are the controls adequate? What could fail? Once the right questions are posed, appropriate answers can be found or readily determined from studies keyed to sound engineering judgment.

The responsibility for overall safety is shared by all; however, this responsibility increases with each echelon of supervision and management, until it finally focuses on the "top man." Safety program implementation just doesn't happen; it can only be done in the style and to the degree that top management supports the program.

Safety necessarily involves the assessment and acceptance of certain minimum levels of risk. Management in its decision-making processes must have visibility of the residual risks and alternatives attendant to on-going operations. Hazards and the means for their control must be clearly identified, considered in appropriate trade-off studies and displayed to the management approval chain.

#### COMPLEX R&D OPERATING SYSTEM; LEWIS RESEARCH CENTER

For the present purposes of discussion, the complex R&D ground operating system (referred to in the title) will be the NASA-Lewis Research Center. As an operating system, we will be referring to all in-house Center R&D plant operations. Hopefully, the safety principles and organizational approaches employed here may find interest and application to other field installations or other complex, potentially hazardous operations.

Let's first examine this particular field installation! The Lewis Research Center's R&D mission (figure 1) is focussed in three broad areas; (1) advanced propulsion systems, (2) energy

and power generation systems for both terrestrial and space applications and (3) launch vehicles (primarily applications of the [LH<sub>2</sub> - LO<sub>2</sub>] Centaur stage in support of the unmanned space science programs). Included is the entire spectrum of airbreathing, chemical rocket and electric propulsion systems. Approximately 55% of the Center's resources are used in support of the aeronautics program. Essentially, Lewis is a gas-turbine engine, related technology laboratory! The attendant diversity of potential hazards is truly enormous; for example, there are hydrocarbon fuels, cryogenic fuels and oxidizers, high-voltage plasma rigs, submicron powders, high-pressure and high-temperature structures and containment vessels, hard vacuum systems, high-speed rotating machinery, radioactivity, toxic materials, etc. Subsequently, it will be shown that 650 to 700 separate and diverse activities have been identified as being hazardous and are under safety permit control.

The Center's physical plant covers some 350 acres and is shown in the aerial photograph of figure 2. Probably the most unique, distinguishing characteristic of the Lewis Research Center is its central air process system. This is in evidence in the photograph by the large (five- to six-foot diameter) overhead lines that distribute combustion air (up to 450 psi) and altitude exhaust to the furthest extremities of the Center. The prime movers for this system are 5- to 20,000 horsepower compressors and exhausters located in two main buildings---the Engine Research Building and the PSL Equipment Building. From this central air system, approximately 50 to 60 different research customers have process air conditioned and admitted to their research rig or facility. With some components more than 30 years old, the system was designed for versatility, economy and efficiency. In its operation, there is a high degree of flexibility achieved by the manual setting of valves to route the conditioned air to appropriate facilities; of course, there is an attendant price in complexity and hazard! This process air system is operated around-the-clock on a three-shift basis. To maintain order and efficiency, it is important that detailed and effective scheduling of facility operations be accomplished.

Other major facilities that are identifiable in the aerial photo are two propulsion wind tunnels (a 10-by-10-Foot Supersonic Wind Tunnel with speeds from Mach 2 to 3.5 and an 8-by-6-Foot Supersonic Wind Tunnel with speeds from transonic to Mach 2). The PSL buildings include four altitude tanks in which full-scale jet aircraft engines are operated under various conditions of simulated pressure altitude. Program support aircraft are operated out of the hangar. In the upper right hand corner are two large space-environment facilities for evaluating electric propulsion systems in simulated space flight conditions. There is also a zero-gravity facility

which consists of a vacuum chamber approximately 20 feet in diameter and 500 feet deep in the ground with a pneumatic accelerator located at the bottom. (On an up-and-down trip, experimental packages can achieve approximately 10 seconds of zero-gravity conditions.) There are some 140 structures at the Center with a plant value of about 300 million dollars.

Of course, one cannot run a plant and facilities such as these without people! The general array of personnel functions necessary to operate and manage such facilities are indicated in figure 3. The Center has a total complement of approximately 3,050; of these, approximately 1,350 are professional scientists and engineers. As indicated in the wheel chart, each major facility must operate with people organized in different functional groups. It is vital that effective communications and delineation of roles be achieved in order to establish a true safety awareness among personnel. Training must be an essential and integral part of the safety program.

#### PROGRAM APPROACH AND ORGANIZATION

The Center then is made up of people and facilities! This is the investment that we must protect. The Lewis safety program cornerstones are identified in figure 4. As indicated, safety must start at the top with management support and visibility of the residual risks encountered in day-to-day operations. The safety program must reside on the sound engineering judgment of its most experienced and knowledgeable people. We have required that there be an overall systems approach adopted to the review of individual operations. We must recognize the responsibilities of the R&D line management and at the same time achieve a parallel review channel reporting to top management. In effect, we are to establish a third-party review process. It is essential that we have visibility and control of operations. In our case, this is done with a paper system--the so-called "safety permit" system. The permit is a paper that stipulates the restrictions, precautions and requirements for operation and, thus, becomes a basic training and communication document between the technicians (who do the work) and the researchers (who generate the requirements). Obviously, a certain amount of safety documentation must be established and maintained.

In organizing the safety program, the Center plot plan was subdivided into seven geographical areas with boundaries established as indicated in figure 5. Each area includes a complex of facilities with some degree of operational similarities and requirements. Within each, six to eight knowledgeable experienced people are ap-

pointed by the Center director to form an area safety committee. By design, the membership of the committee is interdisciplinary in its makeup. These members serve on a part-time basis (perhaps, 10-15% of their time on safety reviews and apart from their prime job assignments such as in research or operations. These area safety committees report to an executive safety board. The functions of the area safety committee are to effect the third-party review and to issue the safety permits. The permit is a paper reflecting the concurrence of the area committee on the proposed safety plan and is simply a clearance to operate or to proceed with the activity. The executive safety board is responsible for the promulgation of safety policy, to resolve any impasse between the line and the area safety committees, and to provide visibility to the Center director of the overall safety posture of the Center. Functional advisory panels are also made up of specialists to coordinate and work with the various area safety committees. There are two standing accident investigation committees to determine facts and recommend corrective actions on accidents/incidents as they arise. The safety director is responsible for the operation and management of the Lewis safety office and wears an extra hat as the executive secretary (or the implementing arm) of the board.

### THIRD-PARTY REVIEW AND APPROVAL PROCEDURES

A flow chart of safety approval procedures is illustrated in figure 7 for Lewis in-house operations. As discussed earlier, the initial burden of developing the safety plan rests with the cognizant project engineer (PE). It is his function to bring his proposed plan to the area safety committee for detailed review. Should there be established precedence and all questions and challenges pertaining to safety resolved, then a safety permit will be issued and the project engineer will find his activity clear to operate. However, if there are additional findings or unanswered questions by the area safety committee, there may be several iterations between the area safety committee and line management before issues are resolved and a safety permit issued. Impasse and significant major risk assessment are to be passed on to the executive safety board and, in certain cases, major elements of risk or cost are referred with recommendations to the Center director for resolution. Keep in mind that there is an effort to restrict membership within the area safety committee to personnel outside direct line management responsibilities--so that, in effect, we don't have people reviewing their own work. In this way, we effect a third-party review parallel to the line. Ultimate responsibility and resolution of impasse rests at the Center director level.

## SYSTEM SAFETY

Much has been bandied about in the literature relative to "system safety." Some confusion and, perhaps, suggestion of mystique (or cultism) seems to hang over it, particularly when one attempts to define system safety as being something apart from industrial or institutional safety, aviation safety, public safety, etc. If one accepts the definition of system safety as suggested in figure 8, ---"a reasoned approach---logic based on facts and engineering judgment---a systematic study to identify all potential hazards and to determine means to effectively control or eliminate the hazards," then system safety is the name of the game and adequately describes our approach to Lewis in-house operations.

System safety tools/techniques can be useful in analyzing, focussing, displaying and dealing with potential hazards. Some are listed in figure 8 and are defined herein in the Appendix. Complexity of the system will obviously determine the depth and sophistication of the safety analysis. This is again a matter of judgment; obviously, a simple bell-jar-type activity would not involve as much detail as a full-scale engine in a major test facility. The efficacy of system safety analysis can only be measured in terms of its impact on the decision-making process. As a matter of policy and procedure, an operational readiness inspection (ORI) is required before any new activity is initiated...this is the final check of the system before committing it to operation!

## DEVELOPMENT OF THE SAFETY PLAN

Development of the safety plan is the first responsibility of the project engineer. Elements to be considered in a comprehensive plan are suggested in figure 9. For most operations, the technical literature is replete with safety guideline information in the way of standards, operating manuals, codes, research data and related experience. This is then the safety data bank! In each case, however, the main concern is for the proper and precise matching of environmental parameters found in the cited literature with the proposed test conditions. Here again engineering judgment must prevail! Where appropriate data does not exist, analytic studies and proof testing must be initiated at system, subsystem or component levels.

This perspective on safety standards is further illustrated in figure 10. Operations that are fairly routine or for which adequate precedence has been established can be handled as depicted vertically on the left side of the chart. With appropriate citations

and reference to data bank information, project safety decisions are made through line management with the safety organization (S/O) responsible for monitoring, liaison and technical reviews.

New technology, first-of-its-kind projects with little or no precedent information, must be handled with more detailed physical evaluations as depicted vertically on the right side of figure 10. In these instances, proof-type environmental and stress testing down to the component level must be done in order to reduce the residual risks to a minimum. An important requirement on deviations from conventional or previous related practice is the documentation of the technical justification or engineering analysis. Documentation of successful safety practice becomes guideline information for subsequent similar operations, until with enough experience behind us we can recognize the merit of specific procedures and propose them for consideration as safety standards. An illustration of this might be the Lewis Hydrogen Manual (reference 9) which basically is a compilation of Lewis pioneering procedures and practices in the handling of liquid hydrogen. Documentation of the final decision rationale is essential since it in turn becomes the basis for work specifications and safety rules. It also becomes the training vehicle by which we explain the precautions and environmental constraints to the technicians who are to perform the work.

#### SAFETY PERMIT SYSTEM

In applying for a safety permit, the project engineer must fill out a standardized request form (figure 11 and 11[a]). For hazardous operations, this form is designed to achieve some semblance of uniformity in detailing, categorizing and quantifying the hazard and the proposed safety precautions. Key information would include delineation of environmental test conditions (pressure, temperature, voltage, frequency, flows, etc.), materials problems (chemical compatibility, toxicity, radioactivity, etc.), sensing and detection equipment, emissions and effluents, and specified safety precautions for certain posed situations. An important block to be filled out is the one indicating precedence for the particular type of work; in essence, we don't attempt to reinvent the wheel every time! Signatory blocks are also provided for use by line supervision.

Backup supportive analyses and documentation (including critical system drawings) must be submitted to the Area Safety Committee for review and approval. Upon concurrence of the operating plan, a safety permit (figure 12) is signed by the chairman, issued and posted in a conspicuous place at the operational site. State-



ments on the permit briefly describe the activity and stipulate the safety requirements and the imposed operational restrictions. These safety specifications then become required basic training for the supporting technician staff, who are under instructions not to perform work outside the scope of or not covered by a safety permit. All permits must be renewed and updated at least annually.

Because of the great diversity of hazardous activities around the Center, each safety permit is color coded to provide a quick ready reference for plant protection personnel who might be called in to fight a fire. The code simply specifies as follows:

Green: (No unique firefighting techniques are required.)  
Take action - use Water, Dry Chemicals or CO<sub>2</sub>.

Yellow: (Fire involving liquid metals, high voltage, etc.)  
Take action - use DRY chemicals ONLY.

Red: (Unique - potential high explosive, high toxicity, nuclear radiation, etc.)  
Take action ONLY after advice of a knowledgeable person (i.e., project engineer).

In all cases, copies of current safety permits are also maintained by the plant protection staff and become an integral part of their building inspection patrols and pre-fire planning exercises.

To track the safety permits for operational location and currency, an automatic data processing (ADP) system is inputted by local supervisors (Technical Services Building Managers) and monthly printouts are provided. A sample page of the Facilities Utilization Report is shown in figure 13. For each building and room around the Center, operational tasks are described along with safety permit coverage and expiration dates. Safety concerns and utilities available to the area or room are also designated in accordance with the legend at the bottom of the page. Expired permits are removed from the site and the operations or work stopped, until renewal is effected through appropriate channels.

#### CENTER SAFETY OVERVIEW

A representative monthly report summary is shown in figure 13 (a). In effect, we have a compilation of known hazards and a snapshot of the operational status for the many rigs around the Center! For example, at this particular time there were 380 high-voltage/high-amperage operations, 94 hydrogen rigs, 22 activities employing

450 psi combustion air, 158 operations using natural gas, etc. Of the 1136 activities reported, 103 are designed for unattended operations. There were also 104 permits that would expire within this reporting period. This Facility Utilization Report is an excellent operational tool for the building manager and provides some overall top management visibility of the safety program.

With a great range and diversity of operations occurring in a relatively congested area, proximity factors become important in considering the potential for chain-reaction effects, wherein one accidental failure (or energy release) can, in turn, trigger yet another accident. A cursory "domino effects" study (based on Armed Services Explosive Safety Board quantity-distance criteria) was made of the Lewis fuels, oxidants and gas storage depots (as shown in figure 14). Separation distances, personnel evacuation zones and barricades to remove line-of-sight shrapnel were evaluated for conformance to standard practice and Center policy. Further detailed studies are required. With the level of complexity, other potential paths for accident propagation are open and must be taken into account in achieving a systems approach to all safety reviews of Center activities.

#### EMERGENCY CONTAINMENT TEAM

Personnel available to aid in emergency containment are shown on figure 15. The first echelon to combat any engineering situation is the in-house plant protection staff consisting of 24 full-time personnel who are charged with manning firefighting equipment and emergency vehicles. Their backup, second-level reserves are auxiliary emergency reaction teams, consisting of 50 other employees who are trained in emergency rescue, firefighting and first aid techniques and are assigned on-call emergency support roles via their job descriptions. In a major fire (or aircraft accident), municipal (or airport) fire-fighting forces would also be called in. In personnel injury situations, the Lewis Medical Services (a full-time doctor and two nurses) are available.

How do we insure that the emergency team performs as a well-oiled machine? One general observation that seems to prevail in the aftermath of most accidents is that a written operating procedure or specification had previously existed on paper describing a proper safe way of doing the particular business. It is obvious that the mere generation of paper does not in itself constitute a safety program. It is but a step!

## PROJECT "STEEP"

In most instances, accidents involve people--human frailties, errors of omission or commission. Safety instructions too often are not read, or read but soon forgotten. To circumvent this shortcoming, Lewis safety training policy is aimed at achieving an aggressive continuing program of instruction and exercise (or dry-run emergency drills) tailored to the needs and activities of particular divisions. Such are the objectives of Project STEEP (Safety Training in the Execution of Emergency Procedures) as represented in the logo of figure 16.

Project STEEP is aimed at developing the team concept in achieving an efficient fast response to posed emergency situations. It requires delineation of roles to be carried out among interfacing groups working in a given area; e.g., mechanics and engineers. Simulation drills will be conducted and designed to exercise the "teams" in appropriate procedural details. A system of communications is all important! The range of STEEP activities might include such exercises as the use of the emergency call system, area evacuation procedures, first aid and heart resuscitation techniques, general housekeeping, fire-fighting, explosion protection, operations in emergency protective gear such as the Scott air-pack, radioactive or toxic releases, etc. These must be coordinated efforts between Plant Protection, Medical Services, the Safety Office and the line organizations.

Examples of planned, organized emergency simulation training exercises under Project STEEP are shown on figure 17. The first rule in any emergency is to effect a rapid orderly building evacuation of all personnel. The response is timed, evaluated for procedural deficiencies and reviewed post-facto with the designated evacuation monitors. Key operating personnel are trained in first aid and cardiovascular resuscitation. Mock disaster exercises are held to review these techniques and to put into practice personnel rescue procedures. To simulate an actual case, hot fire drills are conducted periodically. Here, plant protection crews work out with "light water" (AFFF) hoses on a gasoline pool-type fire. Emergency reaction team members also participate in the hot fire drills (as do municipal firefighters, at times) and learn to operate the emergency equipment. Here you see them throwing water and running flow tests on the equipment.

## CONCLUDING REMARKS

In closing, the effectiveness of any safety program must rest

on the support of management and the interest and motivation of the employees. It must be so ingrained in everyone's mind as to be recognized as the only way to effectively accomplish the business. Sound engineering judgment has to be the backbone of the safety decision-making process. While documentation and paperwork (figure 18) in itself doesn't make a safety program, a certain amount becomes essential in providing top-management visibility of the safety issues and the residual risks in operations. It is, perhaps, most important in working with unique high-energy R&D facilities, such as we have discussed here. Essential safety documentation can probably be best defined by post-accident investigation criteria. Simply, how well were the risks recognized, considered, sized and managed? At Lewis, the Executive Safety Board minutes are the prime vehicle for safety overview information. It is the means by which management obtains some visibility of residual risks in its overall plant operations.

## APPENDIX

### SYSTEM SAFETY TOOLS/TECHNIQUES

As extracted from the referenced literature, the following assurance tasks are defined herein to clarify terminology and to illustrate the logic and analytic methodologies of system safety:

- Hazards Identification and Criticality Ranking:

An examination is made to determine all potential hazards that might be the result of inherent properties or characteristics of equipment, material or human failures, or environmental stresses. It includes consideration of the interrelationships of primary, initiating and contributory hazards and all pertinent circumstances involved in system operations. Hazards are then categorized in order of criticality, such as (1) potential loss of life, (2) potential mission failure, (3) delay or loss of operations and (4) excessive unscheduled maintenance.

- Preliminary Gross Hazards Analysis:

In the initial phases of development (e.g., siting considerations for hazardous operations or facilities), significant energy sources are identified, quantity-distance criteria are taken into account and methods are selected for containment and control of these energy sources.

- Worst Case Analysis; Maximum Credible Accident:

A system in its operational lifetime is exposed to environments, processes, conditions and loads of varying magnitudes. The stresses and effects produced will differ at various times. All of these and their interrelationships are analyzed for the worst case conditions that could exist, the most serious hazards, and the most damaging effects that could be produced. The term Maximum Credible Accident is employed to indicate the worst-case condition that can reasonably be expected to occur. The probability may be extremely low, but not so low that it would be impracticable to incorporate suitable safeguards in the system.

- Design Reviews; Fail-Safe Design Philosophy:

This is the independent review and determination of the adequacy of design with respect to its

intended functions. This review activity should be performed on both a continuous and discrete basis. Safety aspects of the design which are deemed inadequate are subjected to a disciplined procedure of responsible follow-up to assure that corrective action is taken, documented and verified for efficacy. Special problem areas within the design are reviewed and trade-off studies initiated as required to solve these problems. Documentation of the design review is required with a complete list of all action items resulting from the review. Design reviews should be conducted at various points during the design; a preliminary design review during the early stages of design, a critical design review near the end of design, an operational readiness review, and a final design review after the equipment has been placed in operation plus informal design reviews throughout the program. The design reviews provide project engineering and program management with the necessary visibility to determine problem areas actual or potential, as well as possible resolutions to these problems.

Since failures will occur, fail-safe arrangements are another means to prevent disabling of a system or to prevent a catastrophe involving major damage to equipment, injury to personnel or degraded operation. Fail-safe design insures that occurrence of a failure will leave the system unaffected or converted to a state in which no injury or damage can result. Fail-safe designs can be categorized into three types:

- (1) Fail-passive arrangements reduce the system to its lowest energy level.
- (2) Fail-active design maintains an energized condition that keeps the system in a safe mode until corrective action occurs.
- (3) Fail-operational arrangements allow system functions to continue safely until corrective action is possible.

#### Development Test Analysis:

Design uncertainties are resolved and design decisions are finalized by a means of the results of development tests. The development test program (including the test procedures

as well as the test results) is an excellent source of system effectiveness, strength and efficiency information. This analysis should be a vital adjunct to the system effectiveness assessment activity.

● Failure (Hazard) Mode and Effect Analysis:

This is a system analysis which is initiated in the early stages of design and considers the mode (function), the mechanism (hardware/software) and cause (chemistry, physics or human) of possible failures together with the effects of such failures on the system operation, consequence of failure to the system objectives, probability of occurrence for each possible failure, deterrents to obviating the failures from occurring, and all corrective action required to prevent the failures from happening. A tabular analysis is prepared for systems, subsystems, components or parts. It is initiated in the early stages of development and/or design but is continually updated throughout the life cycle. During early conceptual studies, this analysis is used to delineate, in order of severity, those critical functions and related hardware which can lead to specific consequences to given mission objectives and/or crew/personnel safety. During the developmental phase, the F(H)MEA is a primary tool for design evaluation. The analysis is later used during the test phase as an input for checkout procedures and test emphasis as well as fault isolation. In the operational phase, the F(H)MEA aids in selection of alternate modes of operation under primary failure as well as in preparation of both prelaunch and inflight diagnostic procedures. Logistically, the analysis finds application in determining allocation of spare parts and selection of field personnel.

● Fault Tree Analysis:

This graphic analysis traces by means of Boolean symbology the relationship of all minor events which contribute to the occurrence of a major undesired event in a system. This analysis has two major elements. The first is the logic diagramming, known as a Fault Tree, which connects by means of "and" and "or" gates events (known as sub-events) which contribute to the terminal undesired event of interest. The second element consists of the subevents themselves. These subevents are normally limited to the "what" of an incident rather than including how, why, who or where. While the FTA is a decisionary tool, it is primarily a motivational tool during early system conceptual activity. The full merit of the FTA is not real-

ized until the development phase because the branches of the Tree cannot be traced to sufficient depth to influence design. During this phase, the emergency of certain paths as being more critical than others causes designers to revise their approach. A unique purpose of the FTA is to provide a system view of the impact of an undesired event, thus allowing every person who contributes to a system to see and understand how they might be consequential in an undesired event.

● Life Testing:

A comprehensive test technique, life testing examines and verifies the deleterious effects of long term steady-state operation of equipment. Also, the testing verifies the effects of storage and shelf-life aging of components. Both life testing and stress testing should utilize statistical design-of-experiment techniques in test planning to facilitate objective analysis of the significance of varied test conditions upon the parameters tested and to maximize information per dollar from test programs. Good techniques to compress life testing in a meaningful way are needed. The specific purposes of life testing are to demonstrate the life expectancy of the hardware under normal operating conditions of load and environment; to determine the effects of storage of the hardware in a nonoperating mode under actual or simulated storage environments; and to determine the shelf-life of the hardware considering non-metallic materials aging, lubrication deterioration or loss of lubrication, metal migration, and other related factors.

● Environmental Stress Testing:

This test technique is applicable to system elements which are more sensitive to environmental stresses than to long-term operation. Design margins are determined by means of testing to failure under specified conditions of stress. This approach is applicable to those items which are not destroyed at each level of stress in order to observe their response(s). Stress testing relates failure rates to operating stresses under controlled or measured environments. The stress environment must represent the true environment to provide meaningful results. These data are used as inputs to establish functional relationships between failure behavior and associated parameters under various time and stress conditions. Then, the functional relationships are utilized for comparative evaluations of new processing techniques and new device types, realistic initial and end-of-life specification limits, and parametric prediction of



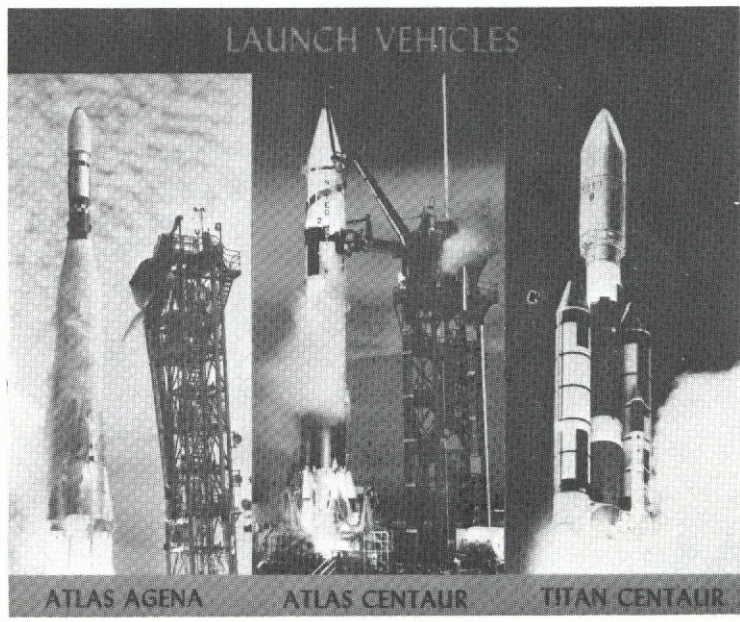
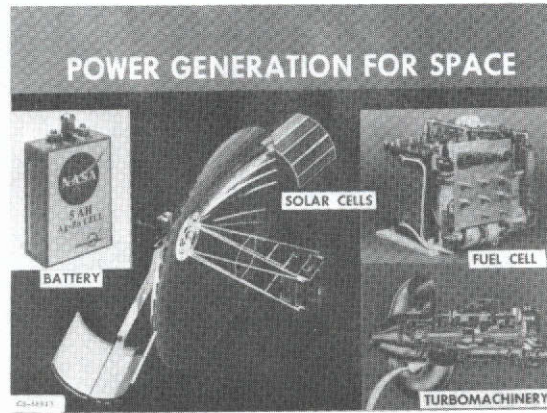
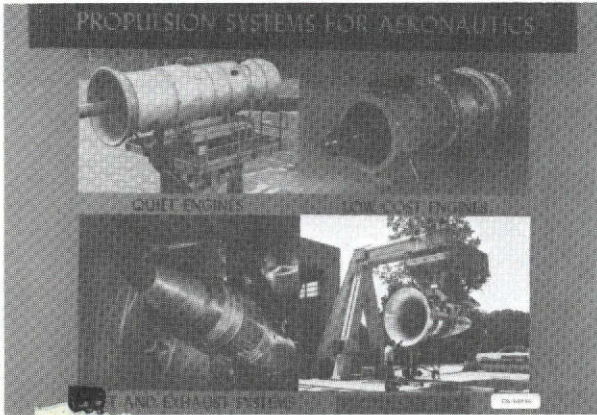
failures.

● Trade-Off Studies:

This task covers the establishment of system effectiveness requirements and capabilities in various times during the system engineering process. A uniform and identifiable process is required for logically comparing total system effectiveness regardless of system purpose, size, or complexity. This task must produce quantitative or probabilistic results if it is to be a decision-making tool. The measures of effectiveness should be based on mission objectives. These measures, together with other comparisons such as total system cost, are used as inputs to the decision-making process for choice of best alternative. This occurs at all stages of the system engineering process that is a part of every new or upgraded equipment acquisition and operation. Trade-off studies completed in the concept definition phase are used to arrive at the best concept. Major decisions are made at the system level as to which concept is the most feasible in terms of effectiveness, cost, and all other criteria necessary for decision. Trade studies are used during system definition phase to aid in selection of the best alternatives for use at the subsystem and component level, and during design definition to design level decisions.

## REFERENCES

1. NASA Safety Manual. Volume 1: Basic Safety Requirements. NHB-1700.1, National Aeronautics and Space Administration, 1969.
2. NASA System Safety Manual. Volume 3: System Safety. NHB-1700.1, National Aeronautics and Space Administration, 1970.
3. Enthoven, Alain C., Dr.: Hearings before the Subcommittee on Government Operations. United States Senate, Ninetieth Congress, First Session, Sept. 27 and Oct. 18, 1967.
4. Ball, Leslie W., Dr.: "First, Catch the Rabbit..." System Safety Newsletter, Volume 3, No. 3, 1974, pgs. 1-6.
5. Grose, Vernon L., Tustin Institute of Technology, Santa Barbara, California: Top Management System Safety Course at LeRC, April 30 to May 4, 1973.
6. AIAA Technical Committee on System Effectiveness Tasks, presented at Annual Reliability and Maintainability Conferences, June, 1971, and January, 1974.
7. Hammer, Willie: Handbook of System and Product Safety. Prentice-Hall, Inc., 1972.
8. Lewis Research Center in-house Operational Safety Manual.
9. Hydrogen Safety Manual. NASA TM X-52454, 1968.



81

Figure 1 - LEWIS RESEARCH CENTER R&D MISSION

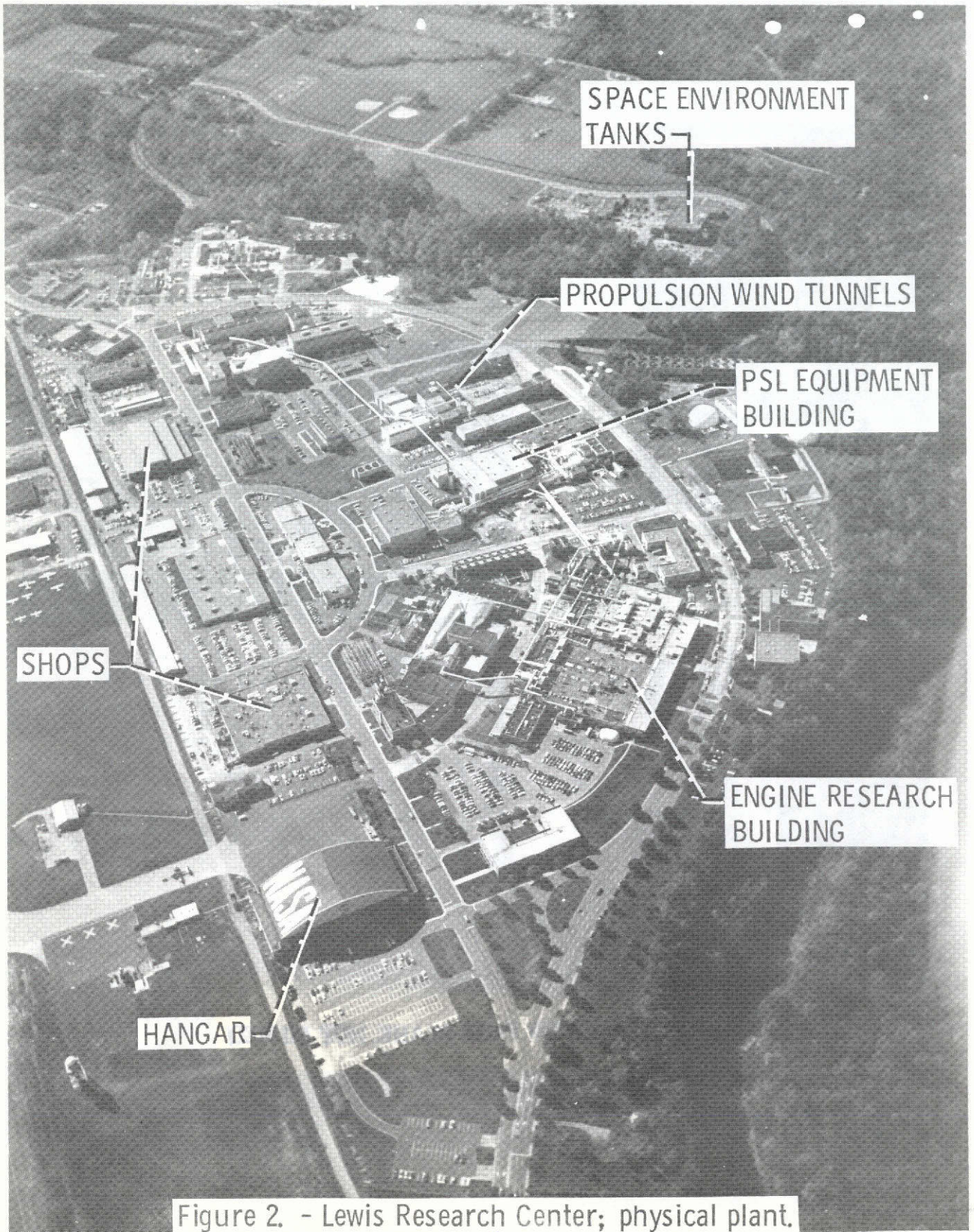
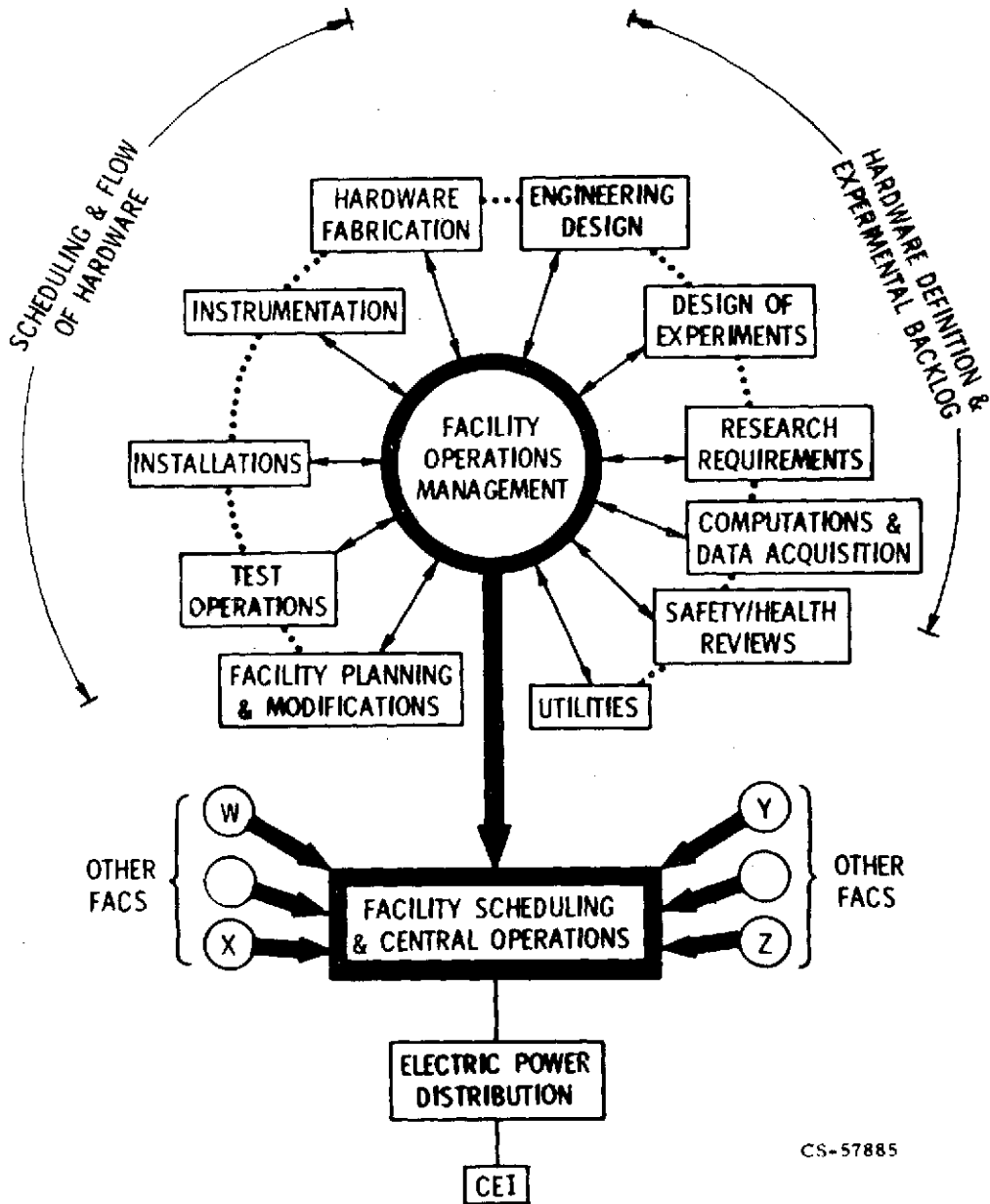


Figure 2. - Lewis Research Center; physical plant.

Figure 3

### FACILITIES MANAGEMENT



CS-57885

20

Figure 4

SAFETY PROGRAM CORNERSTONES

- Center safety policy and organization
- Top management support and visibility
- Decision basis; sound engineering judgment
- Systems approach
- Third-party reviews
- Safety permit control of operations
- Safety training and communications
- Safety documentation

Figure 5

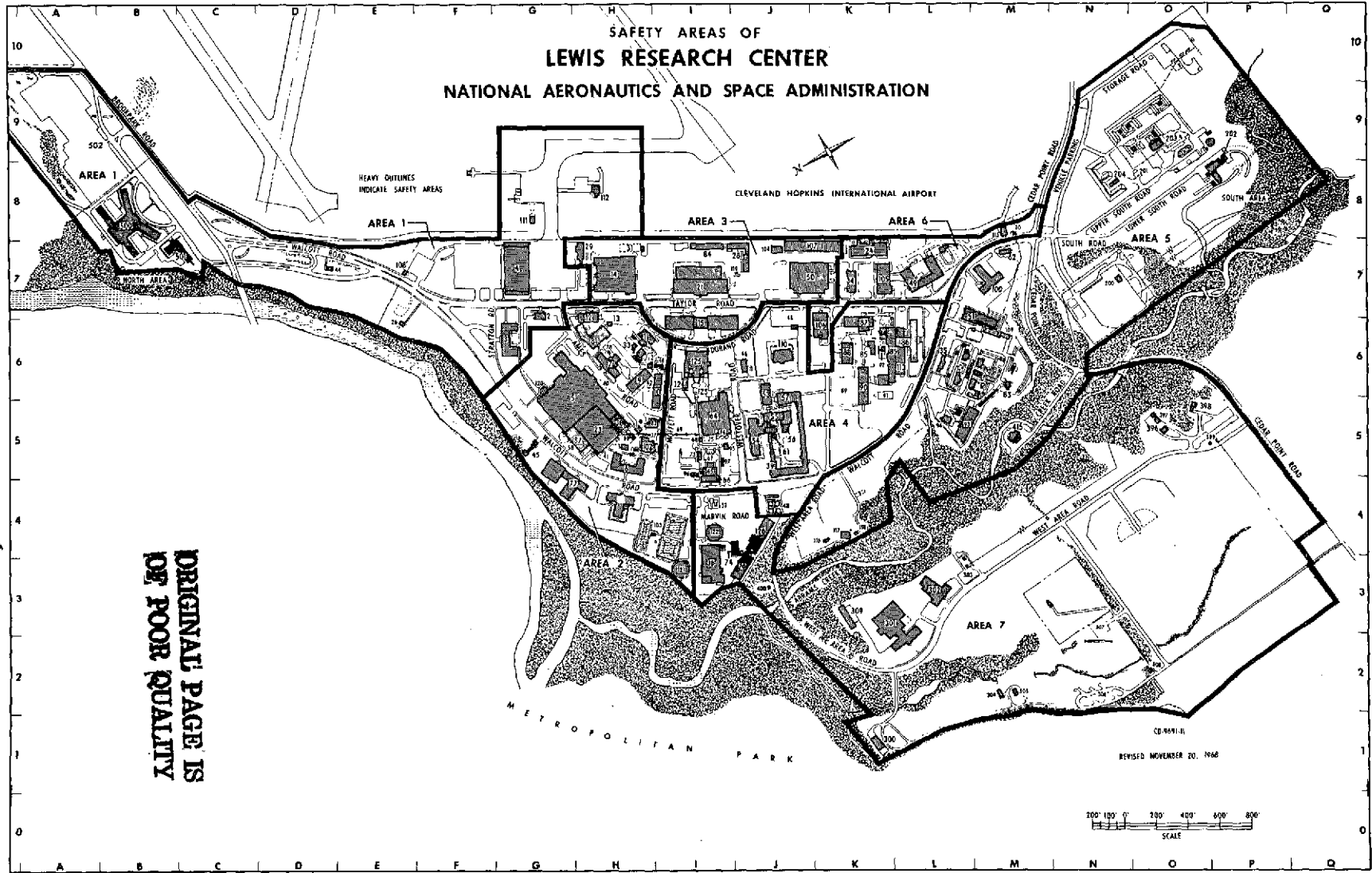


Figure 6 - LEWIS SAFETY ORGANIZATION

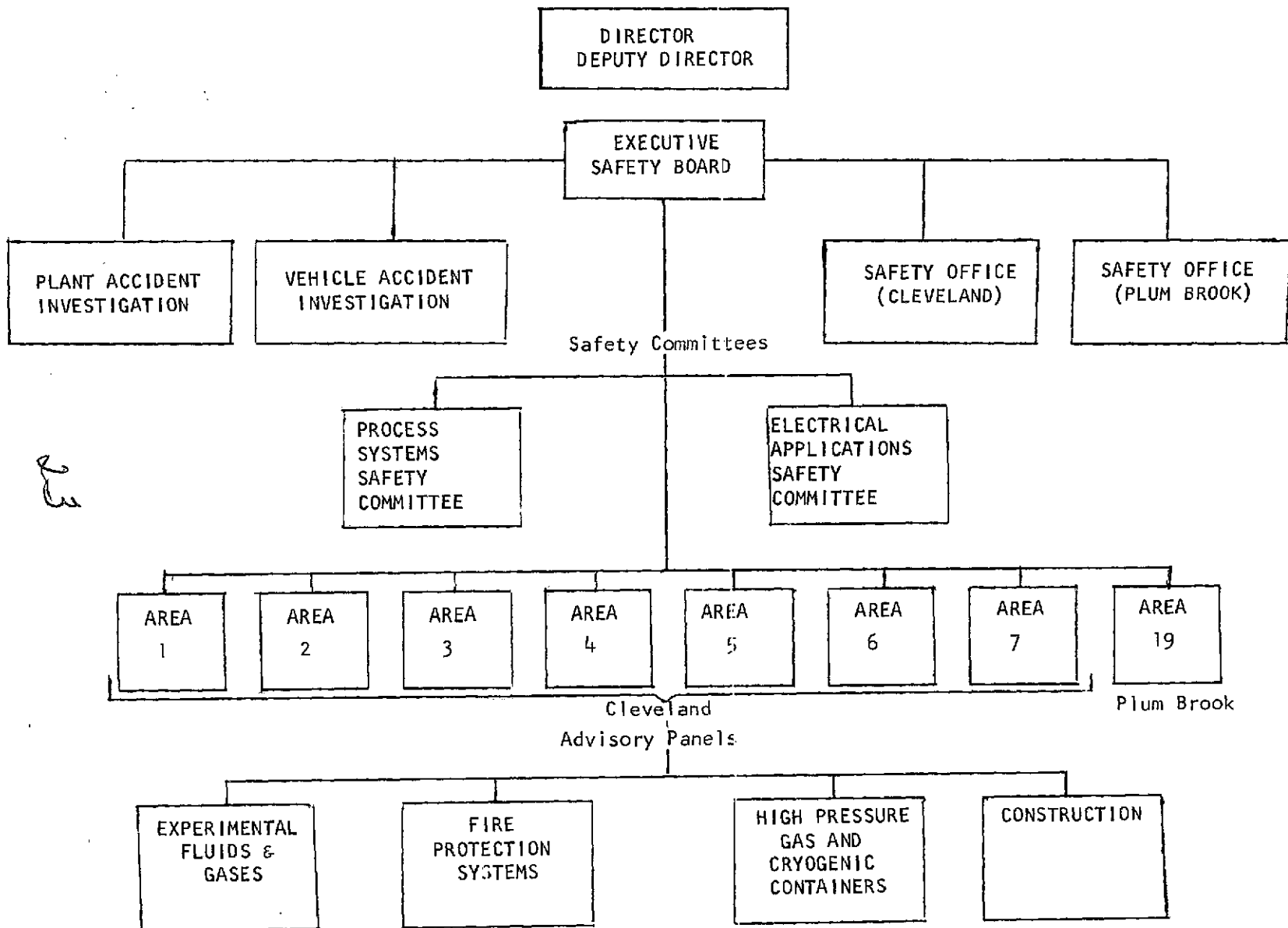






Figure 8

SYSTEM SAFETY ANALYSIS

- a reasoned approach or logic based on facts and engineering judgments to define clearly the safety issues and alternatives for effective decision-making
- a systematic study to identify all potential hazards and to determine means to effectively control or eliminate the hazards

SYSTEM SAFETY TOOLS/TECHNIQUES

- Hazards identification
- Preliminary gross hazards analysis
- Worst case analysis; maximum credible accident
- Design reviews; fail-safe design philosophy
- Development test analysis
- Failure (Hazard) Mode and Effects Analysis
- Fault tree analysis
- Life testing
- Environmental stress testing
- Trade-off studies

25

Figure 9 - ELEMENTS INVOLVED IN A COMPREHENSIVE SAFETY PROGRAM

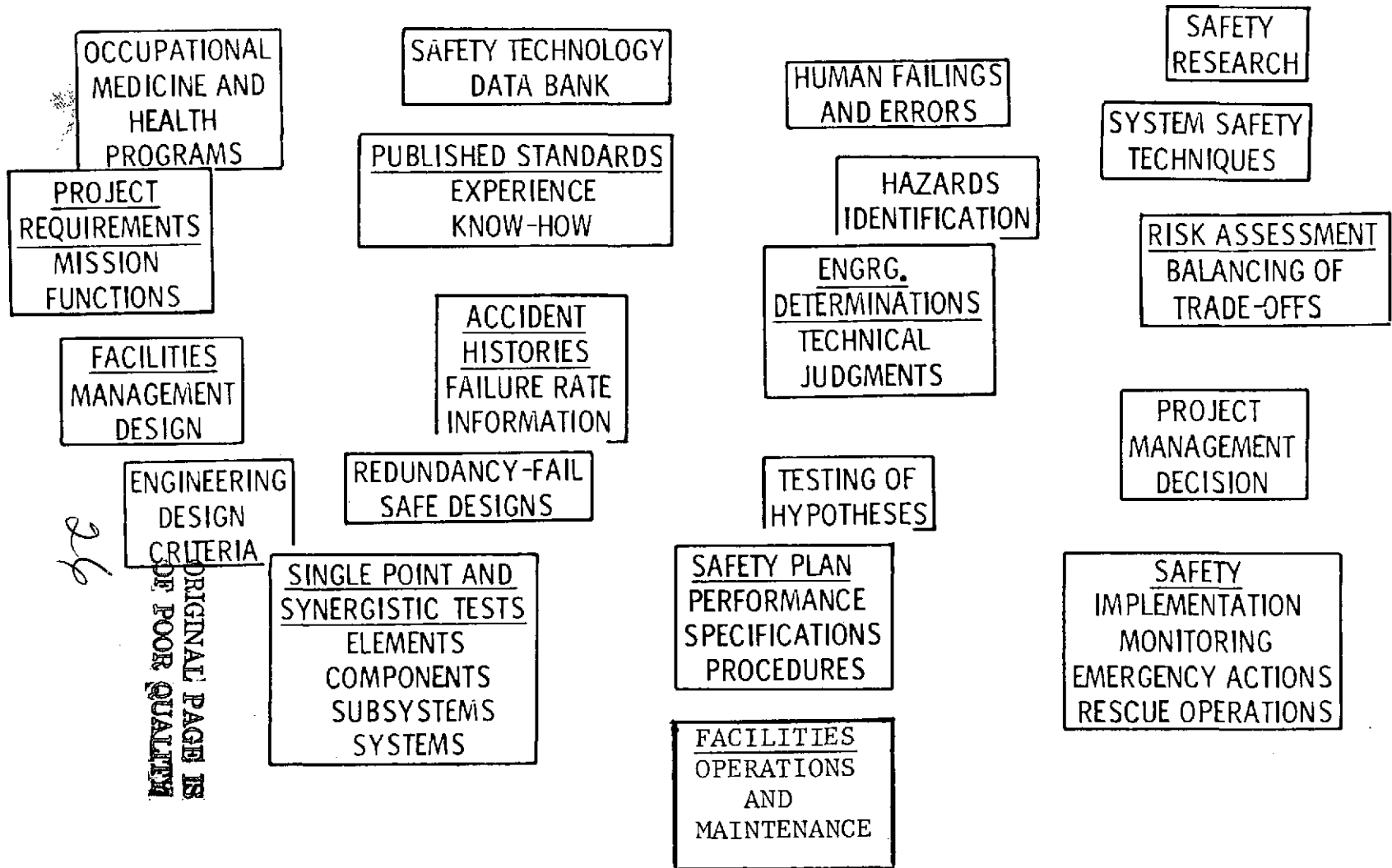
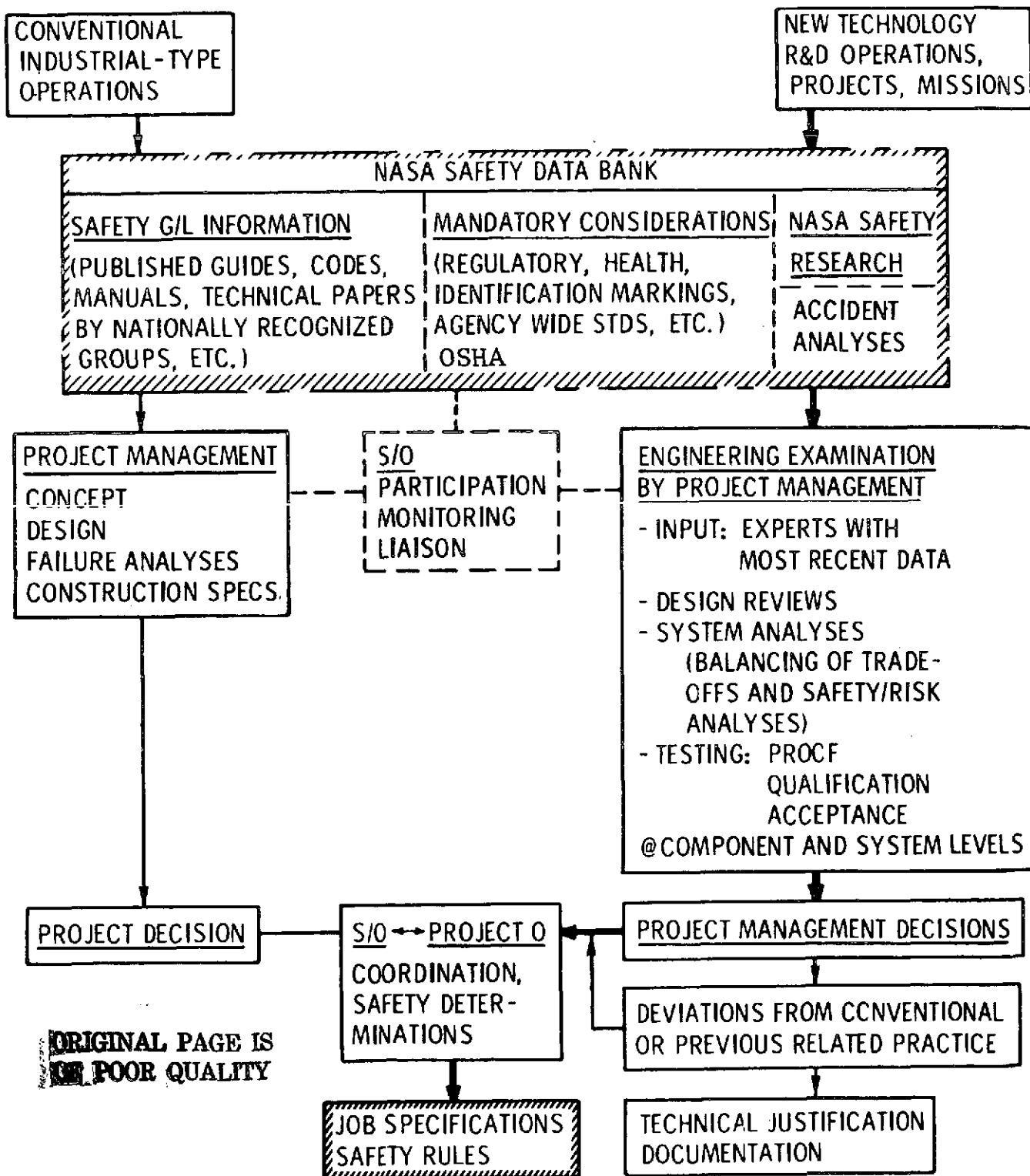


Figure 10 - PERSPECTIVE ON "SAFETY STANDARDS"



ORIGINAL PAGE IS OF POOR QUALITY

S/O = SAFETY ORGANIZATION  
G/L = GUIDELINE

27

Figure 11

<b>SAFETY PERMIT REQUEST</b>		<b>SAFETY COMMITTEE USE ONLY</b>	DATE	Permit No.	
				PREVIOUS	
				NEW	
<p><b>INSTRUCTIONS:</b> Prepare and send one copy of this form to each as shown. If required (see LMI 1703.1), attach pertinent drawings, hazard analysis and Users and Experience Record (NASA-C-197) for:</p> <p>Cleveland requests: Lewis Safety Officer Area Safety Committee Chairman Area Safety Committee Reviewer Plant Protection Test Installations Division Project Engineer (Responsible Engineer)</p> <p>Plum Brook requests: Lewis Safety Officer Area Safety Committee Chairman Area Safety Committee Reviewer Safety Officer at Plum Brook Facilities Service Division Project Engineer (Responsible Engineer)</p>					
T O	<input type="checkbox"/> AREA SAFETY COMMITTEE NO. _____				
F R O M	PROJECT ENGINEER NAME (Responsible Engineer)	ORG. CODE	PAX	PBX	MAIL STOP
1. ACTIVITY (Describe research operation, facility, equipment, etc., requiring safety approval.)					
2. LOCATION (Room, building, cell, etc.)		3. DRAWING NOS.		4. WORK UNIT NO.	
5. TESTS (Nature of objectives, etc.)					
6. EXPECTED DURATION DATES			7. TEST RUNS		
START _____			LENGTH: _____		
COMPLETE _____			TIME: <input type="checkbox"/> WORKDAY <input type="checkbox"/> NIGHT <input type="checkbox"/> WEEKEND		
8. TEST CONDITIONS (List the most hazardous conditions; use of fluids, power, radiation, etc.)					
MATERIAL, FLUID, ETC.	VOLTAGE, PRESSURE, ETC.	FREQUENCY, TEMPERATURE, ETC.	QUANTITY		REMARKS
			AT SITE	IN RIG	
9. MATERIALS DESCRIPTION ("X" Blocks for materials to be used.)					
<input type="checkbox"/> TOXIC		<input type="checkbox"/> CORROSIVE		<input type="checkbox"/> EXPLOSIVE	
<input type="checkbox"/> PYROPHORIC		<input type="checkbox"/> RADIOACTIVE		<input type="checkbox"/> OTHER (Specify) _____	
10. DESCRIPTION OF RADIATION AND/OR RADIOACTIVE MATERIAL (Complete and attach Users Radiological Training & Experience Record (NASA-C-197) for each user.)					
PHYSICAL FORM:		TYPE OF RADIATION:		ELEMENT OR COMPOUND _____	
<input type="checkbox"/> SEALED SOURCE		<input type="checkbox"/> ALPHA <input type="checkbox"/> GAMMA		ELEMENT OR COMPOUND WEIGHT _____	
<input type="checkbox"/> UNSEALED SOURCE		<input type="checkbox"/> BETA <input type="checkbox"/> NEUTRON		RADIOACTIVE ISOTOPE _____	
<input type="checkbox"/> GAS		<input type="checkbox"/> OTHER (Describe, if such as X-ray producing equipment.)		WEIGHT % RAD. ISO. IN ELEMENT/COMP. _____	
<input type="checkbox"/> LIQUID				ACTIVITY CURIES _____	
<input type="checkbox"/> SOLID					
11. RADIATION DETECTION INSTRUMENTS					

ORIGINAL PAGE IS  
OF POOR QUALITY

28


Figure 11(a)

<p>12. IS THERE A PRECEDENT FOR THIS WORK? (If "Yes", give details.)</p> <p><input type="checkbox"/> YES _____</p> <p><input type="checkbox"/> NO _____</p>	<p>13. NASA-C-197 (attached) <input type="checkbox"/> YES <input type="checkbox"/> NO</p> <p>(Name) _____</p>		
<p>14. DISCHARGE PRODUCTS (Radioactive, corrosive, combustible, toxic and air/water pollution materials.)</p>			
<p>PRODUCTS (Temperature, Quantity, Radioactive, Etc.)</p>	<p>MEANS OF COPING WITH DISCHARGE PRODUCTS</p>	<p>FINAL DISPOSAL MEANS</p>	<p>REMARKS</p>
<p>15. SAFETY PRECAUTIONS (Indicate what provision has been made for the following typical items.)</p>			
<p>SITUATION</p>	<p>SAFETY PRECAUTION</p>		
A. Ventilation			
B. Detection of hazardous condition (Radiation, toxicity, etc.)			
C. Ignition sources			
D. Safe location of personnel during tests			
E. Avoidance of unsafe contamination of fuel or oxidant			
F. "Fail-Safe" means in case of power, pressure, combustion or personnel failure			
G. Protective means in case of over-temperature, over-pressure, or over-speed			
H. Accident Procedure (Fire, explosion, spill)			
I. Collapse of vessel from evacuation			
J. Personnel protection (Protective clothing, breathing apparatus, medical check, etc.)			
K. Grounding			
L. Guarding of live parts			
M. Shielding (Radioactive material, radiation producing equipment, and high frequency radiation)			
N. Hazard - warning signs			
<p>16. SPECIAL ITEMS (List pertinent items peculiar to conditions of proposed test)</p>			
PROJECT ENGINEER (Signature)	DATE	SUPERVISOR (Signature)	DATE

29

Figure 12

NOTE: COPY OF SAFETY PERMIT REQUEST MUST BE POSTED WITH THIS PERMIT.

 <h1 style="margin: 0;">SAFETY PERMIT</h1>	SAFETY AREA <b>2</b>							
	PERMIT NO. <b>2-1238</b>							
	DATE ISSUED <b>7-11-73</b>	EXPIRATION DATE <b>7-11-74</b>						
	WORK UNIT NUMBER (TASK) <b>YOL 4822</b>							
	REPLACES PERMIT NO. <b>2-1150</b>							
LOCATION (Room, building, cell, etc.)  <b>SE-7, ERB</b>	DRAWING NOS. <b>CD-502891</b> <b>CF-500873, CF-502887,</b> <b>CF-502886. Layout and</b> <b>installation diagrams</b>	(Affix color coded sticker here.)  <b>NASA-C-919c (9-68)</b>  <b>This color is . . . GREEN</b>  <b>TAKE ACTION</b> <b>USE</b> <b>Water, Dry Chemicals, or CO<sub>2</sub></b>						
ACTIVITY (Describe research operation, facility equipment, <u>provided</u> , safety approval.) <b>AUTOMOBILE ENGINE EXHAUST EMISSION STUDIES</b> An automobile gasoline engine with various emission control devices drives a dynamometer. A max. of .2 gpm of gasoline is supplied to the engine from a 1000 gallon trailer parked outside the cell. A max. of 10 SCFM of H <sub>2</sub> gas may be supplied to the engine from the H <sub>2</sub> distribution system. A max. of 2 SCFM of a H <sub>2</sub> -CH <sub>4</sub> gas mixture may be supplied to the engine from a bottle located outside the test cell. The cell ventilation is supplied by a 10,500 CFM fan drawing air in from the basement and cell and exhausting to the roof. Flow of H <sub>2</sub> and H <sub>2</sub> -CH <sub>4</sub> to the cell is limited by sonic flow orifices. Engine exhaust is water-cooled and ducted to atmospheric exhaust. Up to 4 SCFM of engine exhaust gas is passed thru various emission analyzers located in the control room and ducted outdoors. The analyzers use span gases containing trace amounts of CO, CO <sub>2</sub> , CH <sub>4</sub> , and C <sub>6</sub> H <sub>14</sub> in N <sub>2</sub> from the cylinders located in the fuel storage room. Zero gas is N <sub>2</sub> . A H <sub>2</sub> generator supplies a max. of 200 SCC/min. for the flame in the HC analyzer.		<table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td>EMERGENCY CONTACT <i>(Knowledgeable person)</i></td> <td>HOME PHONE</td> </tr> <tr> <td><b>P. R. Meng</b> <i>(Alternate)</i></td> <td><b>777-8542</b></td> </tr> <tr> <td><b>R. Behrendt</b></td> <td><b>777-0627</b></td> </tr> </table>	EMERGENCY CONTACT <i>(Knowledgeable person)</i>	HOME PHONE	<b>P. R. Meng</b> <i>(Alternate)</i>	<b>777-8542</b>	<b>R. Behrendt</b>	<b>777-0627</b>
EMERGENCY CONTACT <i>(Knowledgeable person)</i>	HOME PHONE							
<b>P. R. Meng</b> <i>(Alternate)</i>	<b>777-8542</b>							
<b>R. Behrendt</b>	<b>777-0627</b>							
<b>ACTIVITY APPROVED FOR SAFETY SUBJECT TO THE FOLLOWING CONDITIONS:</b> 1. The engine installation must be checked for gas/oil leaks before each run. 2. The gasoline supply to the cell must be automatically shut off and the engine shut down in the event of: a. Electrical power failure b. Ventilation system failure c. Detection of gasoline vapor in the test cell or fuel storage room in a concentration greater than one-half the combustible limit. 3. In the case of a gasoline supply line break, the cell ventilation system shall dilute the gasoline vapor in the cell (including basement) to a concentration of less than one-half of the combustible limit.								
SAFETY APPROVAL REQUESTED BY <i>(Project Engineer's name)</i>  <b>Phillip R. Meng</b>								
AREA SAFETY COMMITTEE		ACTIVITY COMPLETED						
REVIEWED BY <b>R. A. Dawson</b> R. A. Dawson	APPROVED (Chairman) <b>E. W. Corsetti</b> E. W. Corsetti	DATE  SIGNATURE						
<b>Area Safety Committee Chairman</b>  After approval of the Safety Permit Request (NASA-C-923), complete this permit in accordance with procedures prescribed in LMI 1703.1C and send one copy to each of the following for:		<b>Project Engineer (Responsible Engineer)</b>  1. Post a copy of this permit, together with a copy of the Safety Permit Request, in a conspicuous place at the location described. 2. Submit a new Safety Permit Request (NASA-C-923) at least 30 days prior to the expiration date if: a. the activity will not be completed by the expiration date; b. any change is made in conditions as described in this permit. 3. When the activity is completed, remove this permit, indicate the completion date, and send it via the cognizant Area Safety Committee chairman through the Office of Environmental Health to the Safety Office.						
<b>CLEVELAND</b> Plant Protection Project engineer (Resp. Eng.) Office of Environmental Health (When applicable) Safety Office	<b>PLUM BROOK</b> Lewis Safety Officer Plum Brook Station Safety Officer Project engineer (Resp. Eng.) Safety & Security Office (P.S.D.)							

30

ORIGINAL PAGE IS  
OF POOR QUALITY





Figure 13(a) - FACILITIES UTILIZATION REPORT

FINAL TOTALS

A-HYDROCARBONS	185	N-CADDE/ADP	106
B-H. VOLTAGE/AMP	380	P-ALT. EXHAUST	72
C-H.S. ROTATION	151	Q-40 PSI C. AIR	70
D-H. PRESS GAS	322	R-125 PSI C.AIR	165
E-OXYGEN	59	S-150 PSI C.AIR	37
F-RADIATION	122	T-450 PSI C.AIR	22
G-MERCURY	81	U-C. T. WATER	131
H-LASER	31	V-IND. WASTE SYS	231
J-CRYOGENICS	276	W-NATURAL GAS	158
K-HYDROGEN	94	X-FUME HOOD	209
L-NITROGEN	314	Y-440 POWER	342
M-TOXIC MATERIAL	186	Z-CO-2 SYSTEM	107
ACTIVE	1136	UNATTENDED OPERATION	103
BUILD UP	134	TOTAL ITEMS	1465
INTERMITTENT	83	TOTAL EXPIRED	104
DORMANT	111	SU-APPROVED	1041
EMPTY	1	SU-NO APPROVAL	379
		SU-NOT APPLICABLE	45

Figure 14 - "DOMINO EFFECTS" STUDY  
 FUELS, OXIDANTS, AND GAS STORAGE AREAS OF LEWIS RESEARCH CENTER

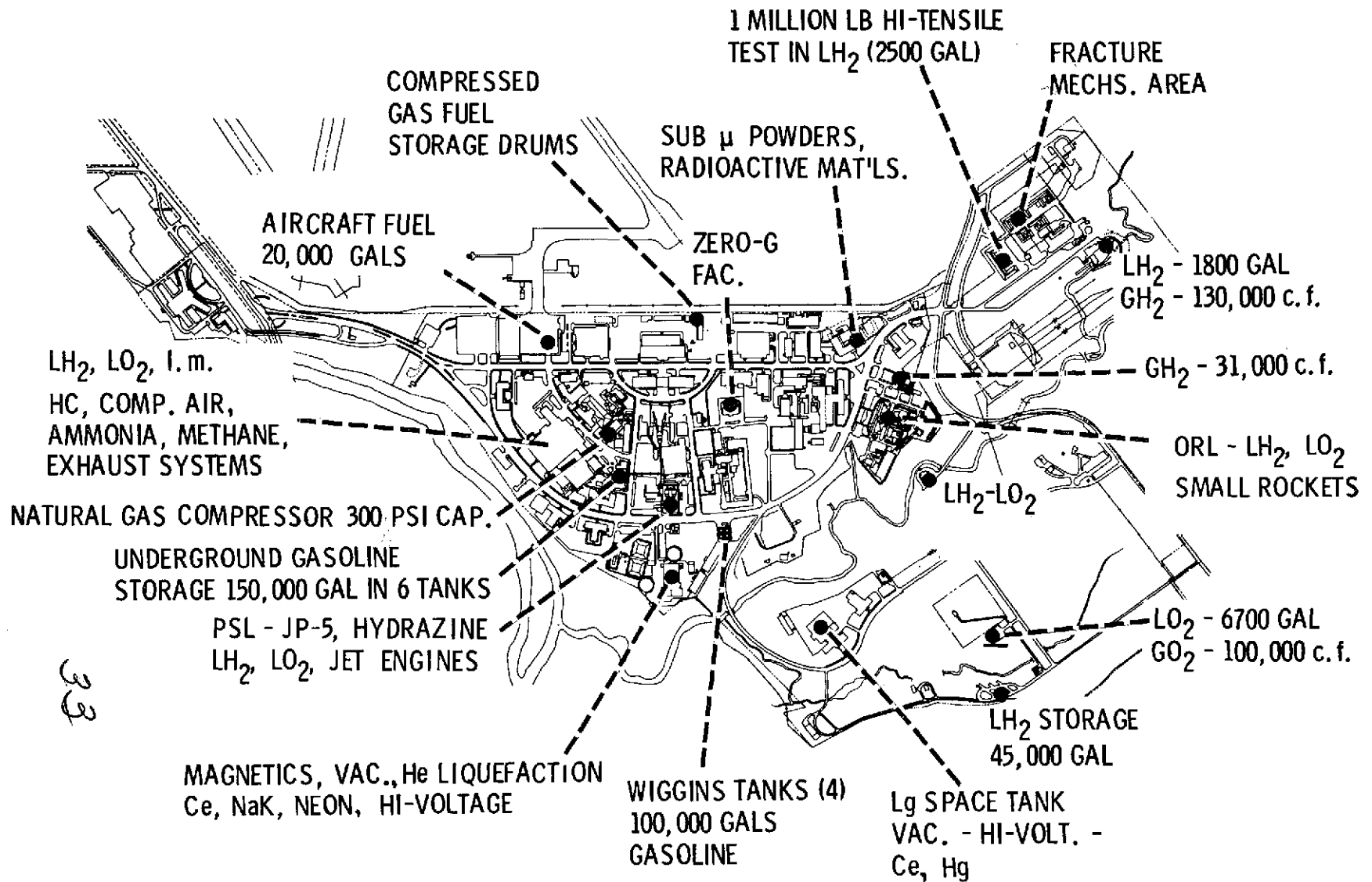


Figure 15

EMERGENCY CONTAINMENT MANPOWER

- In-house Plant Protection Staff (24)
- Emergency Reaction Teams (50)
- Municipal Fire-fighting Forces
- Medical Services (doctor and two nurses)

Figure 16

# PROJECT "STEEP"



LEWIS RESEARCH CENTER

35

Figure 17 - EMERGENCY SIMULATION EXERCISES

BUILDING EVACUATION



MOCK DISASTER



3/6

HOT FIRE DRILLS



ERTS



Figure 18

SAFETY DOCUMENTATION

- Operational Safety Policy (distributed and issued as a Lewis Management Instruction)
- LeRC Operational Safety Manual
- Safe-T-Grams, safety training reports, safety statistics, and accident reporting
- Requests for safety/health operating permits (identification of hazards, analyses, safeguards, and operating restrictions)
- Safety permits (posted in all potentially hazardous operating areas)
- Facility ad hoc committee reports on safety and operations. SAR's.
- Executive Safety Board minutes (management information, coordination, policy, and overview). Overall Center risk assessment.