

2 mif

# NASA TECHNICAL MEMORANDUM

NASA TM X- 64782

## RECORDING AND CATALOGING HAZARDS INFORMATION Revision A

Richard J. Stein  
Safety and Manned Flight Awareness Office

June 1974

**NASA**



*George C. Marshall Space Flight Center  
Marshall Space Flight Center, Alabama*

(NASA-TM-X-64782) RECORDING AND  
CATALOGING HAZARDS INFORMATION, REVISION A  
(NASA) ~~48~~ p HC \$3.25 CSCL 05A

N74-28456

46

Unclas

G3/34 43102

1. REPORT NO. NASA TM X-64782		2. GOVERNMENT ACCESSION NO.		3. RECIPIENT'S CATALOG NO.	
4. TITLE AND SUBTITLE RECORDING AND CATALOGING HAZARDS INFORMATION Revision A				5. REPORT DATE June 1974	
				6. PERFORMING ORGANIZATION CODE	
7. AUTHOR(S) Richard J. Stein				8. PERFORMING ORGANIZATION REPORT	
9. PERFORMING ORGANIZATION NAME AND ADDRESS  George C. Marshall Space Flight Center Marshall Space Flight Center, Alabama 35812				10. WORK UNIT NO.	
				11. CONTRACT OR GRANT NO.	
12. SPONSORING AGENCY NAME AND ADDRESS  National Aeronautics and Space Administration Washington, D. C. 20546				13. TYPE OF REPORT & PERIOD COVERED  Technical Memorandum	
				14. SPONSORING AGENCY CODE	
15. SUPPLEMENTARY NOTES  Prepared by Safety and Manned Flight Awareness Office, Staff Offices					
16. ABSTRACT  Investigating and reporting of accidents is basically a data collection process whose purpose is to discern causation factors of accidents. These factors, once known, lead, in turn, to either the establishment of boundaries or controls aimed at mitigating accident effects or eliminating accidents altogether. A procedure is herein proposed that suggests a discipline approach to hazard identification based on energy interrelationships together with an integrated control technique which takes the form of checklists.					
17. KEY WORDS			18. DISTRIBUTION STATEMENT UNCLASSIFIED-UNLIMITED <i>Leslie W. Ball</i> LESLIE W. BALL Director, Safety and Manned Flight Awareness Office		
19. SECURITY CLASSIF. (of this report)  Unclassified		20. SECURITY CLASSIF. (of this page)  Unclassified		21. NO. OF PAGES  46	22. PRICE  NTIS

# TABLE OF CONTENTS

	Page
SECTION I. SUMMARY . . . . .	1
SECTION II. INTRODUCTION . . . . .	2
SECTION III. STATEMENT OF THE PROBLEM . . . . .	2
SECTION IV. HAZARD IDENTIFICATION SYSTEM . . . . .	9
A. Critical Energy Needs . . . . .	9
B. Destructive Energy Groups. . . . .	15
C. Relationship to Existing Analytical Techniques . . . . .	17
SECTION V. INTEGRATION INTO THE DEVELOPMENT CYCLE . . . . .	19
SECTION VI. FORMS FOR RECORDING INFORMATION . . . . .	21
A. Checklist Forms for Safety Critical Systems Functions . . . . .	23
B. Checklist Forms for Destructive Energy Classes . . . . .	23
SECTION VII. INDEXING . . . . .	26
SECTION VIII. SAFETY POLICIES . . . . .	26
SECTION IX. EXAMPLES . . . . .	26
A. Critical Energy Needs . . . . .	26
B. Destructive Energy Related Forms . . . . .	28
C. Analysis of Functional Areas. . . . .	29
BIBLIOGRAPHY . . . . .	41

## LIST OF ILLUSTRATIONS

Figure	Title	Page
1.	The energy approach to hazard categorization . . . . .	5
2.	Hazard identification system . . . . .	13
3.	Systematic arrangement of hazards catalogue . . . . .	14
4.	Hazard identification relationship of analytical techniques . . . . .	18
5.	Integration of development phases with hazard identification categories . . . . .	22
6.	Critical energy needs . . . . .	24
7.	Hazard identification and control checklist . . . . .	25
8.	Hazard identification planning chart — transportation . . . . .	33
9.	Qualitative relationship of combined environments . . . . .	35

## LIST OF TABLES

Table	Title	Page
1.	Hazard Identification Indexing System . . . . .	7

## RECORDING AND CATALOGING HAZARDS INFORMATION

### SECTION I. SUMMARY

The concept of checklists has been applied universally to jog the memory, as a supplement to recall abilities for accurate or complete performance of functions ranging from mundane activities such as buying groceries to operating aircraft, repairing mechanical devices, or conducting space flight activities. Their forms vary from "you should buy" (shopping lists) to "did you do" or "you should do" (design and operations). They may or may not be aimed at eliciting a simple "yes", "no", or "not applicable" response. However, it is believed that providing for such simple responses for each item tends to ensure that the item is, in fact, considered, and that the information or instruction it contains is applied where needed.

As modern developments progress into more and more complex products, the lessons learned from allied experience or previous analyses become more and more difficult to recall. Thus, the use of the principle of checklists in its more sophisticated applications becomes more demanding and in itself more complex. Retrieval, as well as formulation, becomes of concern and must, if the principle is to find ready application, be easily located and intelligently used. Thus, the system herein described is an attempt to supply a structure for formulating checklists which, of itself, is conducive to practicable retrieval and application by the user.

Checklists can be used for at least four purposes in complex and/or new product development. These purposes are: (1) training and motivation of personnel, (2) conversion of noted conditions and/or situations into languages suitable to specifications and procedures, (3) new product design review and approval, and (4) the support of hazard analyses.

In a more general sense, it is by the assistance of the recorded word that the memory of past things is preserved and the foreknowledge of some things to come is revealed; by words even things inanimate instruct and admonish us. So it is with the checklists. They are only tools, albeit useful tools, in the effort to achieve the basic objective of producing fault-free products, and it is to that end that this systematic approach to analyzing, cataloging, and recording hazard information is directed.

## SECTION II. INTRODUCTION

It has long been recognized that products, especially in the case of new products developed for highly exacting tasks such as spaceflight, must function not only reliably but safely. This latter necessity has focused considerable attention upon activities required to ensure maximum safety, not only to flight crews (in the case of manned flight), but to equipment as well. These activities have evolved a new engineering discipline devoted to identifying hazardous conditions and/or situations. In addition, this discipline ensures that corrective or control measures are implemented by responsible groups. Those hazards that cannot be corrected represent risks which management must factor into their decisions for program continuance or discontinuance.

This brief resume focuses on two vital functions associated with safety; hazards identification and hazard control. The consanguinity of these two functions and the necessity for assuring their comprehensive treatment has prompted Dr. Leslie W. Ball, Director of Safety and Manned Flight Awareness Office, MSFC, to develop the systematic methodology described herein.

## SECTION III. STATEMENT OF THE PROBLEM

Initial steps toward organizing hazard identification and control activities into a universally acceptable system turned toward reviews and analyses of accident histories. This vast reservoir of information was found to be not only subjective, but indiscriminate. Quite frequently the distinctiveness of cause and effect was blurred, frustrating attempts to identify the basic mechanics of accidents. These conditions led to the realization that ordered recording and reporting of accidents was essential if past history and experience were to be preserved for future use. Such considerations suggest a need for a revised approach to accident cause analysis, reporting, and classification, one that would lend itself to universally acceptable logical processes and permit identification of fundamental principles bound up in the chain of circumstances surrounding accidents.

Contemplating accidents creates mental images of fires, explosions, collisions, all of which are symbolic of death, destruction, pain, and/or, in some fashion, unpleasantness. From earliest experience, therefore, the term "accident" associates itself with experiences, ranging from matches singeing the skin to broken bones, all unpleasant experiences that tend to condition mental attitudes toward safety, and generically conceived as

preventing those experiences from recurring. This collage of attitudes inhibits rather than assists the process of dispassionately considering accidents in detached and scientific terms. It also leads to confusing causes, results, and circumstances surrounding accidents and renders of marginal value analytical studies based upon such information. Balanced reflection has led to the conviction that a more effective approach lies in the direction of determining incremental components of accident systems much more accurately than the differentiating capacity of our senses permit; i. e., fire, explosion, collision. It must be remembered, however, that any indirect quantitative determination and any establishment of a systematic approach not manifest to the senses is possible only on the basis of theories. Verification takes place by testing them in all their consequences and finding that they yield concordant results.

For this analysis it is decisive to isolate simple occurrences within the complexity of facts and to dissect the course of events into simple recurrent elements. For the practical viewpoint the system must fulfill the requirement that it reproducibly adapts itself to all situations/conditions as accurately as possible.

Such accidents as fires, explosions, and collisions possess one common denominator, energy. Adapting this concept to a review of accident histories leads to the general hypothesis that essentially all accidents are relatable to energy in one form or another, and suggests that an attempt to classify both accidents and hazards on the basis of energy types and phenomena may very well lead to fruitful results. Reviewing the vast number of accidents reported every day, and pondering the effects of those accidents, leads invariably to the realization that accidents are trisectional in nature when considered as energy mechanisms; high energy, low energy, and energy deprivations. In the high energy class are those accidents reported as fires, explosions, collisions, structural damage, and electrocution. Low energy class accidents are reported as personal injuries (cuts, poisoning, strains, frost bite, and minor burns), and property damage arising from corrosion, termites, strains, and tears. In the area of deprivation of needed energies are physical situations such as entrapment and physiological situations such as suffocation.

Energy has been scientifically defined, studied, identified, and characterized in five distinct regimes; kinetic, potential, chemical, electrical, and nuclear. If these types of energies can be related to accidents, a train of thought may very well be established yielding logical and systematic methods of analyzing information concerning their basic mechanics. It is obvious that controlled energy is the basic ingredient in the caldron of modern civilization

through the devices that make civilization possible. Past developments have been geared to adapting energy to do useful work. Devices ranging from levers and pulleys to internal combustion engines, electrical generating systems and steam engines operate on the principle of exploitation of controlled energy. It is during those occasions when energy becomes uncontrolled that accidents happen. Inherent in every energy-based system is a hazard, the threat of an accident, a means whereby it can inflict damage.

Other situations and conditions arise whose origins lie outside the system but, nevertheless, inflict damage upon it. These may arise from material causes, or induced causes, or they may be of such a nature that the damage is not immediately discernible. That is to say, a time-dependency factor is introduced that may very well delay damage recognition for hours or even days.

In those cases of violent eruptions of uncontrolled energy, the rationalization of the energy-event relationship is readily apparent. Other unwanted situations or conditions arise, however, that test the creditability of the energy approach more rigorously. In the area of controls over critical functions, the energy approach may well seem at first glance to be moot. If, however, the premise is accepted that the control over a function requires the expenditure of energy, an interdependency is defined that only requires verification through application. Two conditions are inherent in these considerations. Framed more descriptively, they may perhaps be formalized as (1) potentially destructive energy sources and (2) energy capability needs. The first group is conditioned by the term "potential," reflecting the fact that any system containing concentrated energy possesses the potential for inflicting destruction under certain circumstances. The second group recognizes that energy is required to perform work, which is basic to the physics of mechanics. Considering work as a function, energy capability is needed to perform a function. If the function is denied its normal energy requirements or if an excess demand occurs by any one or a combination of several mechanisms, the function will not be performed. Thus, if the needed energy is not met and the function is not performed, a hazard to the safety of the system is in being.

If, for example, the braking system of an automobile fails through the loss of hydraulic fluid, a safety-critical function is lost. Careful consideration of such a situation will reveal that the absence of the means to transmit energy to the brake shoes results in the loss of the braking function. This condition could result from blockage of the hydraulic lines, failure of the mechanical links, freezing of the hydraulic pistons, leakage of the hydraulic fluid, etc. As will be discussed later, these causes are classed as mechanisms that activate the hazard. As another example, failure of a steering mechanism due to a disruption of the means to transmit torsional force to the wheel assemblies results in loss of the directional steering function. Again, a



surge of electrical current to a circuit breaker has on occasion welded contact points and prevented the electrical mechanism from functioning. These and many other similar events indicate an area of concern in which accidents have occurred because of a deficiency or an oversupply of energy disrupting a critical function.

Careful consideration therefore, allows a generalization of the part energy assumes in accident systems; first, in its uncontrolled and destructive release, and second, in its role relative to safety-critical functions (Fig. 1).

Acceptance of these two principal hazard-energy interdependencies is the key factor in developing a classification system in the detail necessary to permit practicable use as an analytical tool for identifying hazards. Considering those situations in which discernible destruction occurs leads to the realization that the energy originates from sources within the destroyed object or conversely from sources outside the destroyed object. In addition, destruction can take place in a nonviolent manner at a rather measured pace suggesting minor, though important, energy activities. Collecting these considerations into a formalized statement leads to the establishment of three subgroupings involving the release of destructive energy: (1) High-Energy Environments (sources originating outside the object), (2) High-Energy Components (sources originating inside the object), and (3) Low-Energy Phenomena (sources of low order reactivity). It should be noted that (1) and (2) are potentially destructive to all life and property while (3) is potentially destructive only to a sensitive receiver. The laser illustrates these two degrees of potential destruction; the high-energy version projects a beam that will burn everything in its path. The low-energy version projects a beam that is potentially destructive only to a highly sensitive component, which is normally the retina of the eye.

The other major division concerns itself with the disruptions to safety-critical functions by the overabundance or underabundance of energy and has been so designated.

## Constraints

Using the hazard identification categories for identifying energy sources and deprivation/release mechanisms is a rather clear-cut process when dealing in specifics. A class of constraints does exist, and has been encountered, that is so generalized as to constitute policies. The preponderance of these constraints lend themselves very well to inclusion under hazard identification category 1.0 (Table 1), but others may be encountered which seem more applicable to inclusion within either hazard identification categories 2.0, 3.0,

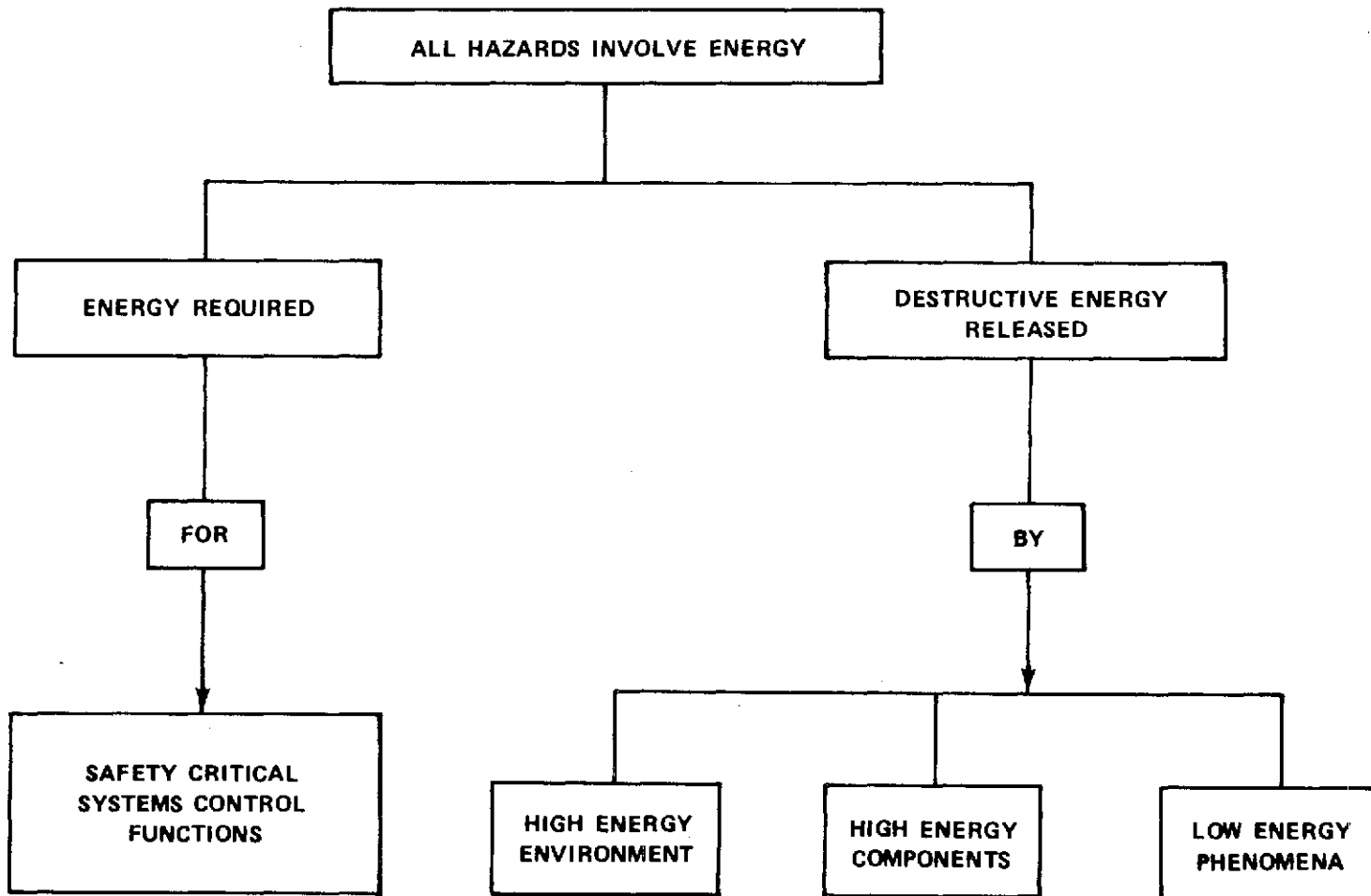


Figure 1. The energy approach to hazard categorization.

TABLE 1. HAZARD IDENTIFICATION INDEXING SYSTEM

1.0	Critical Energy Needs	2.2.4	Projectiles (Meteoroids, Windborne Objects)
1.1	Physical Energy Needs	2.2.5	Temperature (Thermal)
1.1.1	Warning/Abort/Escape	2.2.6	Earthquake
1.1.2	Motion Control	2.2.7	Salt Spray
1.1.3	Information/Command	2.2.8	Pressure/Vacuum
1.1.4	Interface Capability		
1.2	Physiological Energy Needs	3.0	High Energy Components
1.2.1	Human Survival	3.1	Potential Energy
1.2.2	Human Capability	3.2	Kinetic Energy
		3.3	Chemical Energy
2.0	High Energy Environments	3.4	Nuclear Energy
2.1	Systems-Generated Environments		
2.1.1	Dynamic Loads	4.0	Low Energy Phenomena
2.1.1.1	Acceleration Loads	4.1	Toxicants
2.1.1.2	Vibrations	4.1.1	Inhalant
2.1.1.3	Acoustical	4.1.2	Ingesta
2.1.1.4	Pressure/Vacuum	4.1.3	Radiation
2.1.2	Static (Structural) Loads	4.1.4	Absorption (Dermal)
2.1.2.1	Shear		
2.1.2.2	Tension	4.2	Physical Deterioration
2.1.2.3	Compression	4.2.1	Corrosion
2.1.3	Thermal	4.2.2	Embrittlement
2.1.4	Electrical/Electronic	4.2.3	Aging
2.2	Natural Environments	4.3	Physical Contamination
2.2.1	Lightning	4.3.1	Surfaces
2.2.2	Wind	4.3.2	Orifices
2.2.3	Rain (Humidity)	4.3.3	Filters

or, perhaps, 4.0. Each individual case will require its own determination. An example of this situation is the "destruct-system" which may also be considered as a function. In the event the "destruct-function" is constrained, hazard identification category 1.1 should be used for cataloging purposes. If, however, the "destruct-system" is to be constrained, hazard identification category 3.3 should be used. A reasonable approach to such a situation, ensuring retrieval of the constraint, is to include it under one category and reference it under the other. The objectives sought by this system should not be submerged within the mechanics of the system itself. The distinction enumerated above is, therefore, not intended to confuse those using this system but to clarify a situation already encountered and suggest standardized treatment for the sake of consistency.

General policy constraints are, as indicated previously, of a different nature than are specific constraints of specific subjects. The latter quite readily lend themselves to adoption to hazard analysis techniques while the application of the former to hazard analysis may not be so apparent. It is believed that the general policy constraint is more readily useable in conjunction with Fault Tree Analysis techniques. Using Fault Tree rationale permits transmutation of general constraints into specific requirements suitable for inclusion in specifications and procedures.

Additionally, it is recognized that a class of hazards exists that is functional with time, and can be identified through a Time Line Analysis; e.g., the venting of an experimental module that occurs at stated intervals presents a potential gaseous product hazard in the experiment compartment only during that period of venting, otherwise the module is benign insofar as vented gases are concerned. There are many other situations ranging from extravehicular activities (EVA) to transonic (aerodynamic) loading that introduce time-dependent hazards. Using Fault Tree and Time Line Analysis methods, when related to energy-based considerations, offers a very practicable method for exposing those classes of hazards.

As mentioned previously, the unique steps associated with this identification system originate with identification of the energy involvement, proceed to exposing the release mechanism, and then cite control (checklist items) entries that disrupt the potential disastrous interrelationship between the source and the catalyzing mechanism.

Fault Tree and Time Line Analyses are overviews of approach in using general policy and time-dependent constraints for hazard identification.

## SECTION IV. HAZARD IDENTIFICATION SYSTEM

The four categories of energy relations to hazards that lead to accidents are used to structure — categorize and classify safety checklists. The checklist principle itself is the tool by which experience gained from past activities is retained and extrapolated as a guide toward achieving a high degree of confidence that past mistakes are not repeated. It is important to understand that the contents of checklists do not of themselves ensure full fault-free hardware, nor do they replace design judgement in arriving at solutions to engineering problems, any more than a cockpit checklist instructs a pilot how to fly an airplane or a grocery list produces a cook. Designers work every day unaided by checklists, and unless they can appreciate the assistance such a tool offers, they will continue to do so. Thus, checklists must supplement and improve normal capabilities to be effective. In order to achieve the goal of making checklists useful and useable, they have been adapted to the hazards identification system based upon energy considerations. The basic problem in achieving such a marriage of convenience has been relating hazard identification (basically a physics process) to hazards control (basically an engineering process).

The following description, therefore, develops more fully the four categories of hazards identified through energy considerations as well as the system by which they adapt to engineering usage through checklists.

### A. Critical Energy Needs

Energy relationships bound up in accident systems must be pursued definitively along the two general classes discussed previously. It will be recalled that the first of these classes deals with situations in which a controlled expenditure of energy is necessary. Dealing exclusively with this situation, it becomes increasingly apparent that controlled energy utilization is essential to the operability and even to the survival of energy-based systems. On the other hand, uncontrolled energy is destructive. In order to proceed upon this thesis, it is necessary to define systems possessing critical energy needs. Indeed, a little reflection will suggest that all dynamic systems and even static systems possess, in one form or another, the need for energy. In static systems, energy is required to maintain equilibrium; in dynamic systems, energy is required to function. Thus the classification system should be inclusive, and for that purpose advantage may be taken of the classic boundaries separating the inanimate and the animate, the inorganic and the organic, and man and his creations. These have been cast as "physical" and "physiological" systems (Table 1).

Before entering upon an examination of the components of these two all-encompassing categories, it should be mentioned that in applying energy concepts, two basic considerations predominate: (1) those in which demands exceed normal capabilities, and (2) those in which an inability to meet normal demands is encountered traceable to a deterioration of the energy supply. These two basic considerations may serve as guidelines in pondering hazards arising from critical energy needs in either physical or physiological systems.

Turning first to the "physical" group comprising those inanimate static and dynamic systems, four inclusive areas of concern have been identified. These functional areas are: (1) warning, abort, and escape; (2) motion control; (3) information and command; and (4) interface capability.

The first of these functional areas deals with systems used to warn or alert personnel that an undesired event is impending. This may or may not presuppose that sufficient time is available to prevent the event from taking place, but it does presuppose that personnel can escape from its effects. For example, a blinker light placed before a highway construction project can warn the motorist of changed road conditions which may very well be hazardous. At high rates of speed, he may be unable to respond to the warning and crash through the barrier, run into broken pavement, etc.; however, at reasonable speeds, he may stop, detour, slow down, or take action so as to prevent an accident from happening. Again, in the early years of coal mining, miners carried caged canaries into the tunnels to warn them of unsafe atmospheres. The death of the canary warned the miners to leave the area immediately. In these examples, the conditions that could lead to accidents are not removed, but the conditions are advertised so as to facilitate escape from their potential effects. In other cases, alarms and sensors may be used to alert personnel of fires, allowing them adequate time to escape, not necessarily adequate time to extinguish the fire. On the other hand, an alarm on an aircraft indicating engine fire alerts the pilot to the danger so he may take action to save the passengers from mishap. Warning devices are therefore mechanisms used to alert interested parties of hazards to safety as well as dangerous conditions leading to preventive action or timely escape from its effects.

The means for escape should also be provided. Escape systems in their broadest concept range from simple structural devices, such as fire ladders, to the more sophisticated Apollo Launch Escape System (LES).

Abort systems are devices which permit cutting off or breaking off an action, operation, or procedure. In this context, the braking system of an automobile is an abort system in that it provides the means for cutting off the velocity of an automobile.

These three areas are closely related in that they provide the means to alert or warn of impending dangerous conditions, provide the means for breaking off the activities, and the means for escaping the consequences. The use of systems to make these actions possible should be a matter of policy.

Motion control is another function requiring energy, and varies in concept from attitude control of a spacecraft to steering of an automobile. In the latter case, steering an automobile is rather simple under normal driving conditions since the driver is aware of his relative position and where he wishes to go as well as how to get there. In space, steering requires use of a complex coordinate system and equipment to indicate position within that system. Thus, attitude control and steering become vital equipment functions requiring controlled energy. Its area of applicability encompasses the entire mission from lift-off to reentry and landing when applied to space operations.

Information and command are functions closely allied with motion control. Information can be derived from instrumentation systems which measure temperature, pressure, flow rates, acceleration, and vibrations. It can also be secured from the flight crews investigating conditions indicated by telemetry. Aircraft leaving and arriving at modern airfields are controlled and operated through information received from the control tower or associated ground radar stations. Command of vehicles, whether space vehicles or terrestrial vehicles, is exercised by using relevant information of conditions (either external or internal), making decisions, and taking action. The important aspect of this relationship is that the information must be available, timely, understandable, and correct to facilitate execution of the proper command which, in turn, allows proper control of critical functions.

Interface capability reflects concern of the effects one system or its byproducts may have on another or on the entire assembly. Outgassing of a modular payload venting onto other vehicular compartments may cause loss of life if toxics are released, or explosion if reactive gases are released, or serious corrosion of vital parts if corrosive gases are released.

The human, his survival, and preservation of his capability has been of paramount concern to the safety specialist and indeed has prompted a considerable number of laws passed by Congress, the latest of which is the O.S.H.A. act of 1970. A considerable amount of effort has been expended in all areas of society by both the government and the private sector to eliminate conditions that tend to destroy or limit human life, human health, and human capabilities (mental, physical, and sensory). Quite obviously, human life, health, and capabilities are closely entwined, but in this context, human capabilities are taken to mean those capabilities compromised by other than disease, for a human can remain healthy after losing an eye or a limb, but his physical capability is impaired.

Thus, such things as safety glasses, steel-toed shoes, hard hats, and other articles of protective clothing are designed to preserve physical capabilities by preventing or mitigating the degree of injury to the protected parts. On the other hand, sound controlled to acceptable levels not only preserves human hearing (sensory), but may very well preserve his decision-making (mental) capabilities.

In the space program, the concern for human survival is specifically cited in the presidential directive establishing the Apollo Program. Thus, considerable effort has been directed toward ensuring crew survival through supplying critical needs for life support.

Providing for the maintenance of human capability in the space environment has been a much more complex undertaking since the effects of the environment upon the ability of the crew to function have been included in the mission plans to test and establish the boundaries of man's functional capabilities.

The lessons learned from man-in-space operations, his critical life-support needs, and his capabilities form the bulk of experience that should be reduced to checklist form to ensure carryover for future guidance in planning and conducting programs in which man participates.

Returning to the methodology as indicated by the index shown in Table 1, it is unique to this system that an energy loss/excess demand mechanism be identified and present for transposition of the hazard into an undesired event (Fig. 2). Again, three general situations have been used to categorize the types of mechanisms that can activate an accident. They are either unsafe acts, unsafe conditions, or a combination of the two. Unsafe conditions are considered as originating from either design errors or manufacturing faults, while unsafe acts originate from either faulty procedures/practices or from deficiencies in supervisory activity. The identification of the disabling mechanism and its proper categorization as either an act or condition completes hazard identification analysis. Additionally, it is the fundamental factor in developing hazard control measures as checklist items.

Unsafe conditions arising during either design or manufacturing operations are carried forward into the categorization of checklists under eight principal areas in which control may be reasonably expected to be effective (Fig. 3). In this case they are classed as: (1) configuration (safety margins), (2) materials selection, (3) protection or warning devices, (4) interface requirements, (5) fabrication processes or tooling, (6) training and certification, (7) assembly or installation, and (8) inspection or test operations, respectively.



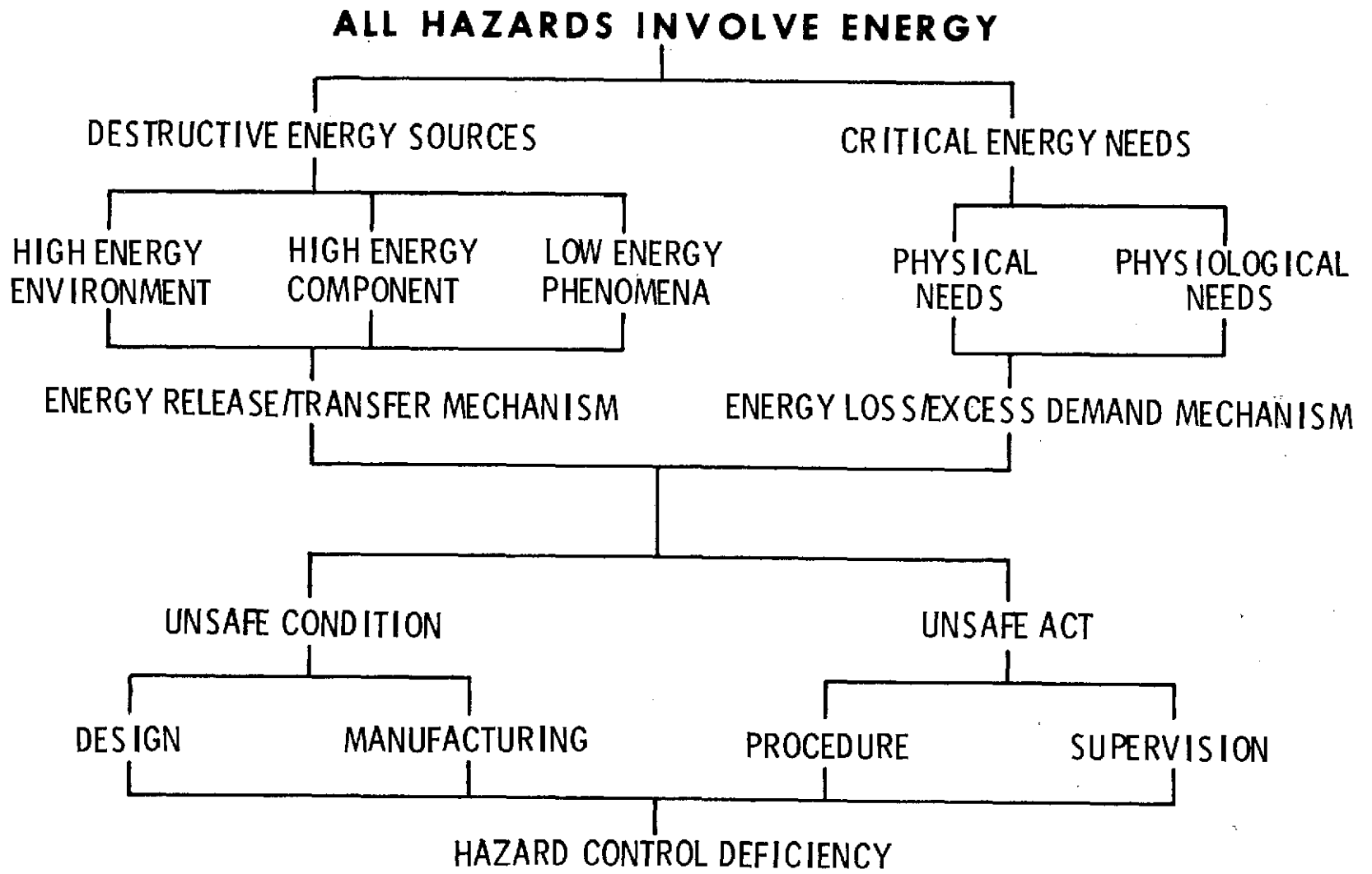


Figure 2. Hazard identification system.

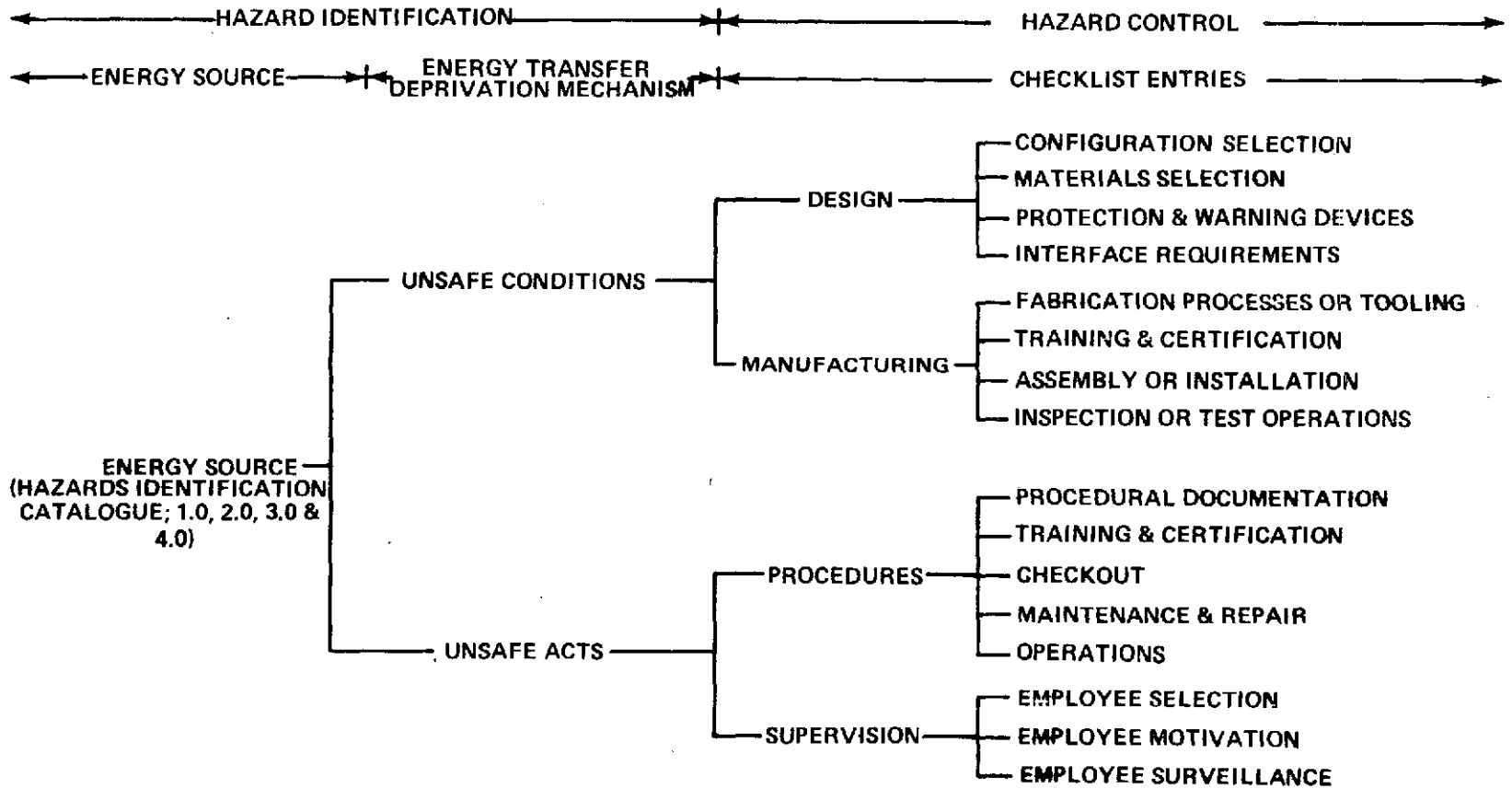


Figure 3. Systematic arrangement of hazards catalogue.

Unsafe acts arising from procedural faults or supervisory deficiencies are carried forward into the categorization of checklists under eight major categorizations: (1) procedure documentation, (2) training and certification, (3) checkout, (4) maintenance and repair, (5) operations, (6) employee selection, (7) employee motivation, and (8) employee surveillance, respectively.

Pertinent control factors, principally in the form of interrogatives, constitute items of the checklist. Cataloging these items under the headings listed above — a total of 15 — only serves as an organizational structure to prompt consideration of all facets that may reasonably be expected to separate or eliminate the disabling mechanism from the source of the hazard identified during analysis.

This rather long explanation has been inserted at this point since it is common to the two major categories of hazards arising from (1) a destructive energy source, or (2) critical energy needs leading to the loss of critical functions. The following paragraphs dealing with the identification of destructive energy sources will, in the case of "controls" or checklist items, follow the same pattern as followed by those identifying "controls" for "critical energy needs."

## B. Destructive Energy Groups

The second grouping under the hazards identification system consists of situations in which destructive energy sources are released, inflicting direct injury or damage. This grouping consists of (1) high energy environments, (2) high energy components, and (3) low energy phenomena.

To repeat again for emphasis, (1) and (2) are potentially destructive to all life and property while low energy hazards, (3), are potentially destructive only to a sensitive energy receiver.

1. High Energy Environments. As previously mentioned, high energy environments consist of those environments induced by the systems and of those attributable to nature. Environments that constitute hazards induced by the systems include acceleration, vibration, noise, temperature, electrical phenomena, pressure, and its antithesis, vacuum. Some examples are launch shock, flutter, engine noise, exhaust flame, capacitor failure, and tank implosion.

Natural environments are lightning, wind, projectiles, temperature, earthquake, pressure, and, again, vacuum. These hazards can create conditions such as stress fracture, fatigue fracture, distortion, electrocution, displacement, fire, and collision.

2. High Energy Components. The high energy component category is self-descriptive since it deals with components that contain, and hence can inadvertently release, high energy. In this case, the energy itself consists of potential, kinetic, chemical, and nuclear energy. These energy sources may be immediately recognizable as basic physical energy classes. Repositories of these energies are pressure vessels, moving automobiles, explosives (conventional), and nuclear bombs. Accidents (catastrophic events) that can result from the release of these energies are explosion, fire, collision, electrocution, and structural destruction.

3. Low Energy Phenomena. Low energy phenomena has been defined as consisting of three sources of hazardous energy:

1. Human toxics introduced into human systems through inhalation, ingestion, radiation, and skin damage. Examples of sources of this type of energy are combustion products, mercury droplets, laser beams, and acid burns.
2. Material deterioration, whose energy becomes identifiable through physical phenomena such as corrosion, embrittlement, and aging catalyzed by exposure to salt spray, hydrogen occlusion in steel, and biological phenomena such as fungus and termites.
3. Physical contamination lends itself to the low energy phenomena category through the idea that, for example, in the case of contaminated optical lens, energy prohibition is introduced through the obstruction of light rays passing through the lens to the focal points. Another association of physical contamination with energy is through the idea that it requires energy to locate the contaminant in a position to produce harmful effects. In still another case of, for example, hydrocarbon contamination of a LOX valve, unwanted energy is added to the system. Additional examples are the results of contamination appearing on surfaces or in fluids/gases and include health damage, orifice (flow) blockage, electrical damage, and bearing seizure. Physical contamination has been included under this headline rather than under functions, since contamination is an identifiable hazard directly associated with hardware rather than a function.

For these three classes of "destructive energy", an energy change must be initiated to initiate a chain of circumstances that leads to an accident.

This energizer has been termed an "energy release" or "transfer mechanism," identical in concept to the disabling mechanism previously discussed. (Fig. 2). Again, as previously mentioned, this energizing mechanism is activated by either unsafe acts or unsafe conditions. This identification scheme is the point of commonality in hazard identification of the two major categories of hazard identification. The "control" phase is also identical to the one previously described.

Observing Figure 2 will perhaps more clearly illustrate the logic of the preceding discussion. In addition, it should be noted that the chain of information leading to hazard identification is based primarily on the physical chemistry or other sciences of the functions/hardware under analysis, while the "unsafe acts/unsafe conditions" as well as control concepts (checklist items) are primarily based on applied science and engineering.

### C. Relationship to Existing Analytical Techniques

The basic concept of the energy-based system for hazards identification lies in the definitive definition of the dual elements of the identification process. If either of these elements is missing, then by definition a hazard does not exist. The concept may be expressed as a "lock and key" system; both are required for functional integrity. It is this definition of the established relationship between energy and its catalytic features that creates the opportunity for integration of all existing analytical safety methodologies within one doctrinaire regime. This consolidation has many advantages, but its principal advantage lies in forming a common frame of reference throughout the discipline of safety. A common frame of reference in turn opens the way for bringing all divergent safety analyses and their results into a single format which facilitates the exchange, retention, and accumulation of pertinent information that is readily comprehended and is thus useable on a wide range of programs and activities. Experience and knowledge recorded in the disciplined manner characteristic of the energy-based system will ultimately produce not only appreciable direct savings but indirect savings in allowing insights into past problems and their resolutions, thereby avoiding costly and marginal false starts leading to catastrophic conclusions.

In the practical vein, the question quite naturally centers on just how can the energy sources and needs be determined and how can the release and deprivation mechanisms be determined. These determinations can be made (Fig. 4) by reviews of technical material in the first instance and by analytical means in the second.

Reviews conducted to determine energy sources and energy needs must consider those sources inherent in the design; that is, those internal to the

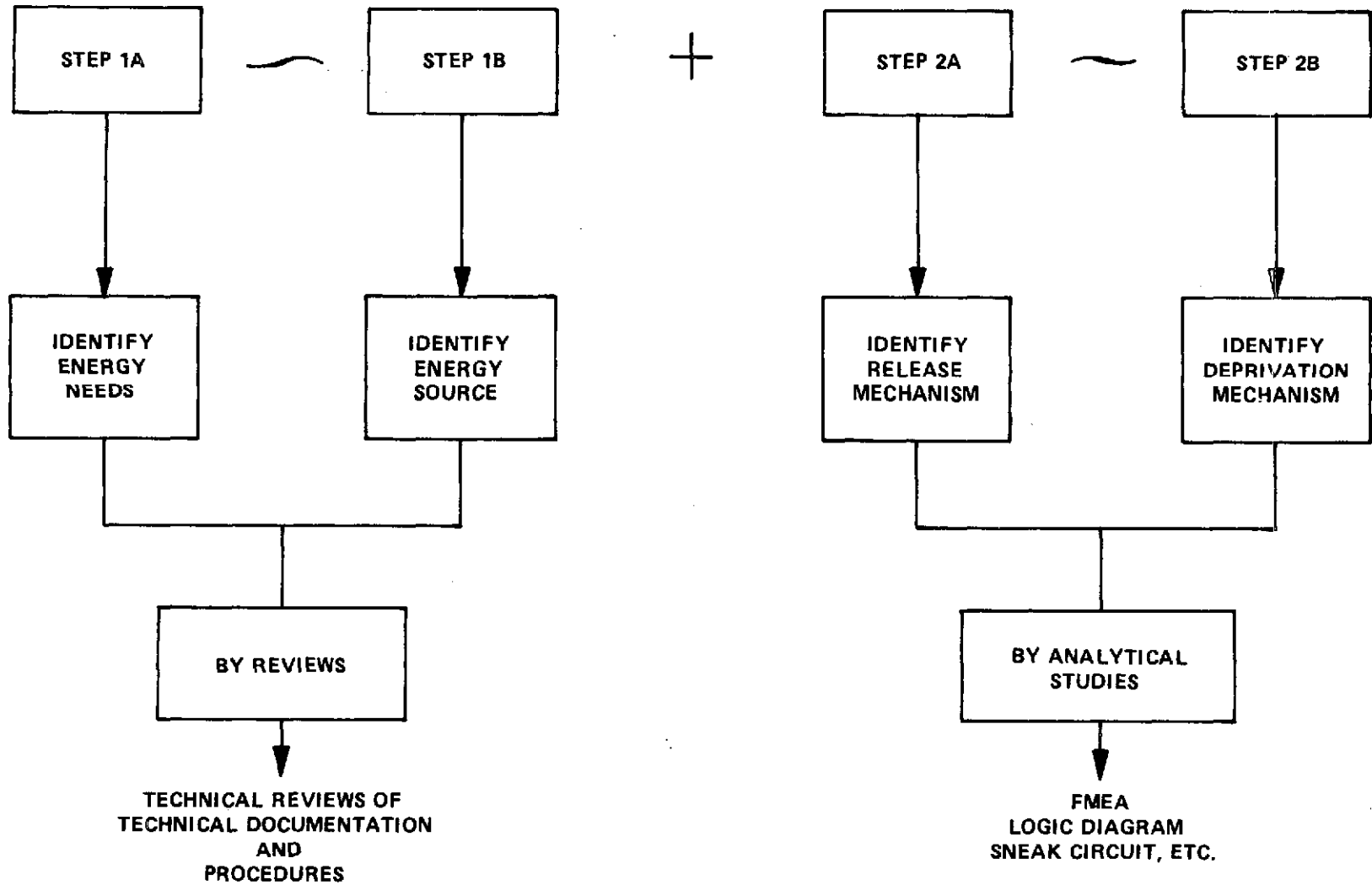


Figure 4. Hazard identification relationship of analytical techniques.

configuration as well as those external sources. Technical documentation, i.e., drawings, specifications, schematics, and layouts, will contain information concerning internal energy sources as well as energy needs. The external sources are possibly more difficult to clearly identify. This case necessitates a thorough knowledge and understanding of the operational features of the design and the medium or environment in which or through which it is planned to move. These may vary considerably from energies associated with aerodynamic characteristics of sonic, supersonic, or hypersonic velocities, to surface conditions of roadways or waterways. In the latter case, for example, icy road conditions may decrease the coefficient of friction sufficiently to affect wheel traction and thereby deprive the vehicle of the energy necessary to come to a standstill. The surfaces of waterways may become sufficiently disturbed by waves, wakes, surface winds, etc., so as to prevent the maintenance of stability necessary to the steering function of vessels. Again, as mentioned previously, a time dependency factor may have to be considered; for example, seasonal changes that influence movement or operations. The external effects of cold, wet, hot, or dry external conditions present unique repositories of energy sources and/or needs.

Thus reviews to identify external energy sources require a knowledge of operations and a knowledge of when, where, and how they are to be carried out.

The energy release and energy deprivation mechanisms (Fig. 4) can be identified by the use of currently available analytical tools, such as the Failure Mode and Effects Analysis, Logic Diagramming, Sneak Circuit Analysis, etc. These tools are generally well known and currently in use. Performed within the context and under the guidelines of the energy-based doctrine they will all contribute similar results even though the techniques vary.

It is not intended that the energy-based doctrine of hazards identification be considered as another of a growing number of methods and techniques available to identify hazards to safety. Rather it should be considered as the system by which all safety analyses techniques can be assembled into an intelligible vehicle by which safety activity can be initiated and carried forward in a milieu of common understanding.

## SECTION V. INTEGRATION INTO THE DEVELOPMENT CYCLE

It is useful to consider development programs in terms of "inputs" and "outputs". In considering how safety and safety requirements are integrated into developments, an interpretation through these two functions may illustrate a satisfactory technique.

The output of a research and development (R & D) program can be envisioned as being in the form of a flow of instructions, each new set of instructions specifying inputs and operations to be performed in them, which will result in a new product of specified attributes. The instructions may be thought of (from the safety point of view) as checklists, itemizing things to do in order to avoid hazards. They relate to the design, development, and operational phases of a new product function. The payoff to the program is the net value of being able to employ these new products, confident that a preponderance of known hazards have been dealt with.

The principal inputs to an R&D program are specialized and trained direct labor (in particular, scientists and engineers); a technical and managerial support staff; equipment and materials used to run experiments, to build and test parts of the whole of the product under development; and various facility items. As implied, the principal safety input is through the efforts of the specialized and trained personnel. It becomes evident, therefore, that steps must be taken to support and augment the levels of experience repositied in those personnel. One technique to accomplish this is through the use of checklists tailored to satisfy their needs in accomplishing safety tasks characteristic of the progress and degree of completion of the development. Since differing tasks and differing concerns are characteristic of the degree of development progress, the necessity of timeliness is quite apparent.

A review of the guideline program planning documentation under which Federal developments are structured clearly reflects this condition by identifying four characteristic phases of R&D programs. Sufficient flexibility has been introduced to allow adoption of the checklist principle at any phase, depending upon the situation encountered. The development phases have been designated as Phase A (concept), Phase B (definition), Phase C (engineering development) and Phase D (operations). A review of the "products" of each of these phases suggests a rough separation between generation of design requirements and generation of design solutions. The first two phases (A and B) are identifiable within the former separation (functional baseline), and the latter phases (C and D) generally align with the (design-to-make-to) products separation. More formally, Phases A and B produce information that is compiled and published as a functional baseline in the form of a program specification. Phases C and D produce a design requirements baseline contained in a Contract End Item Part I Specification and a product configuration baseline contained in a Contract End Item Part II Specification. These phases also produce the experimental hardware that is assembled, tested, and used in accomplishing, demonstrating, designing, engineering, fabricating and operating integrity.



If the energy approach to hazard identification is viewed in the same context, it will be noted that the four groups previously described align themselves into functional and hardware-related categories (Fig. 5). The High Energy Environment category may be considered as transitional since natural environments can be described in nonhardware terms, while their effects act directly on hardware and may thus influence design or selection of systems, subsystems, or components. Hazards associated with functions can be identified by functional analysis quite independent of hardware considerations and thus category 1.0 is relatable to development activities carried out during Phases A and B. As previously mentioned, Phases C and D are hardware related, as are checklist items included in 3.0 and 4.0. Category 2.0 represents a transitional mixture, as previously mentioned, and is thus related to both the "paper" and "hardware" groups.

This suggested alignment of the hazard identification categories and the phases of the Phased Program Development Plan does not imply that these categorized checklists are unique to or can only be used during the development phases indicated, but does indicate where their primary relevance lies. Thus, in early phases when the functions are generally identifiable with particular concepts, those general checklist items cataloged under 1.0 will be found to be of more intrinsic value in hazard identification analysis than perhaps a checklist dealing with a specific component or system. Those checklists concerned primarily with systems, subsystems, and components find their most relevant application to those phases of development where actual designs are converted into experimental hardware. It is believed therefore, that by matching the categories of the hazard identification systems, checklists with the phase of development and integration of subject matter will result from which maximum benefit will occur.

Quite obviously monitoring and controlling safety hazards elimination effort through audits and analyses of work in progress lends itself very well to this systematic approach, highlighting areas of concern and increasing confidence that those areas already considered are adequately treated. Figure 2 shows the transition from "Hazard Identification" checklists to "Hazard Control" checklists. The latter list can be used to generate design criteria for inclusion in the allocated baseline and also for checking compliance of the product baseline and the hardware with these criteria.

## SECTION VI. FORMS FOR RECORDING INFORMATION

The following describes two basic forms on which hazard identification and control information will be recorded.

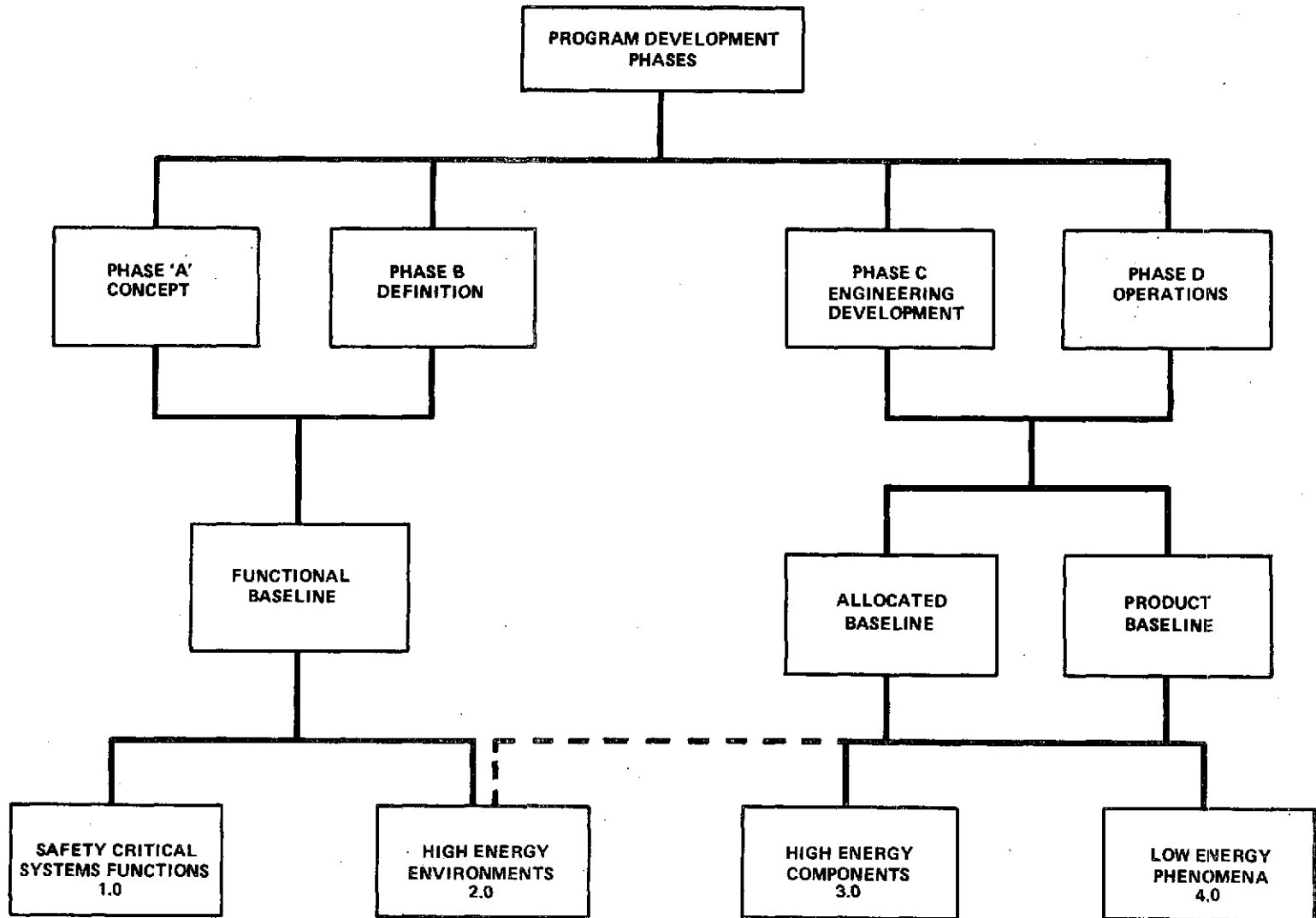


Figure 5. Integration of development phases with hazard identification categories.

## A. Checklist Forms for Safety Critical Systems Functions

A checklist form has been devised (Fig. 6) to collect relevant information for systematic cataloging. Examination of this form reveals, following identifying headings, two major divisions — hazard identification and hazard control. These two functions have been separated so as to aid a safety analyst or practicing engineer in first identifying the hazard and then reviewing the list of requirements aimed at prohibiting the hazard from occurring.

The hazard identification column has been separated into two groups: (1) the hazardous energy source and the controlled energy need and (2) the energy release mechanism/control disabling mechanism. For the purposes of identification, a hazard in each column may be identified as the hazard triggered by either an energy release mechanism or a control disabling mechanism.

The second major division provides space for recording the hazard control (checklist) items under either component critical/procedural constraints or control critical/procedural constraints.

The initial listing of hazards identification and hazards control items is by no means complete. Rather, hazards cataloging is a continuing process of adding, deleting, and refining items on each list.

## B. Checklist Forms for Destructive Energy Classes

The remaining three classes of hazards, high energy environments, high energy components, and low energy phenomena, are recorded on a second form (Fig. 7). Again, it will be noted that the form is divided into two major sections; hazard identification and hazard control. It should be noted that unlike the previous form, hazard identification consists of two major sections — energy sources and energy release/transfer mechanisms, the latter relatable to the disabling mechanism previously mentioned. Following the same pattern as employed earlier, the hazard class will be entered on the form together with its energy source and its release/transfer mechanism followed by hazards control requirements. As a further aid to potential users, the systems, subsystems, and/or components subject to the hazards are also shown on the form. In this case, the hazards control requirements, the checklist items, are cataloged under four major headings: (1) Configuration Design Criteria, (2) Manufacturing Process Criteria, (3) Product Use Procedure Criteria, and (4) Supervision. The completed forms are then filed by system or component to which they are related as a matter of convenience to the user.

HAZARD IDENTIFICATION		HAZARD CONTROL
HAZARD ENERGY SOURCE/ CONTROL ENERGY NEED	ENERGY RELEASE MECHANISM/CONTROL DISABLING MECHANISMS	COMPONENT CRITICAL/PROCEDURAL CONSTRAINTS; CONTROL CRITICAL/PROCEDURAL CONSTRAINTS.

SBAR 369-07-73

Figure 6. Critical energy needs.

CLASSIFICATION _____ ; SYSTEM/COMPONENT _____		
REFERENCE: _____		DATE _____
HAZARD IDENTIFICATION		HAZARD CONTROL
ENERGY SOURCE	RELEASE/TRANSFER MECHANISM	SPECIFICATION/PROCEDURAL CONSTRAINTS

S&AR-36-OT-73

Figure 7. Hazard identification and control checklist.

## SECTION VII. INDEXING

The indexing system used is the standard numerical type (Table 1). This system will be consistent throughout; thus, 2.0 will always be high energy sources and 2.1 will always be system environments.

## SECTION VIII. SAFETY POLICIES

In any development program specific hazard identification and control activities may be guided by constraints that are so general that they amount to policy statements rather than design criteria. For example, a decision to require an ejection escape device for a pilot may be considered either as a development policy or as a checklist item.

## SECTION IX. EXAMPLES

Perhaps an example of each of the two major categories of hazards will serve to clarify how the system of classification works out in practice.

### A. Critical Energy Needs

Example — Guard crewman against excessive radiation from experiment equipment.

Explanation — A cursory review of this requirement indicates that it is not concerned with specific hardware other than the general category of experiment equipment that presumably contains a source of radiation. It is, in fact, a statement of general policy; thus it becomes relevant to the first category of the classification system, 1.0, Critical Energy Needs. In this context it is the goal to preserve the critical human functions by preventing their deterioration through overdoses of radiation which will ultimately lead to death or to serious impairment of human functional systems. Viewed through another light, it may be argued that by preventing radiation overdoses, the system control of the human being is preserved, since any severe deterioration or loss of human systems represents a loss of control of that system, which, in its extreme case, is represented by death.

At any rate, this requirement, as stated, may be logically cataloged as Class 1.0.

Entries on the Form — Turning now to the form (Fig. 6), the first entry, "Classification", should be "Physiological Systems". The date and the references from which the entry originates may be entered as a matter of convenience as well as a source of future information.

The next entries should deal with hazard identification and in the first column the entry "Life Support Human Capability" should be made. This is the control energy need; i.e., to preserve human life and human capability.

The second entry defines the Energy Loss/Excess Demand Mechanism. In this case, the disabling mechanism is "Nuclear Radiation", which would seem sufficiently descriptive to indicate the hazard. With this second entry, "Hazard Identification" is complete.

First, the human crewman has been identified as the subject for which controlled energy (radiation) is needed and secondly, the disabling mechanism (radiation) or perhaps rephrased as energy (radiation) buildup to unacceptable proportions within human systems. The disabling mechanism is the actual buildup or retention by the human systems of radiation doses together with its biological/biochemical reactions commencing when critical levels are reached. If radiation dosage was not cumulative and harmlessly dissipated as fast as it impinged upon the human systems, there would be no disabling mechanism. It should be the objective of those making entries on these forms to be as brief as possible, thus the notation "Nuclear Radiation" would appear to be sufficiently descriptive.

The last column, entitled "Component Critical/Procedural Constraints and Control Critical/Procedural Constraints" is reserved for the requirement (checklist item) for hazard control.

In the example cited, the entry under "Control Critical/Procedural Constraint" may take the form: "Provide crew protection against excessive radiation doses from experiment equipment."

As a note of clarity, if a specific piece of hardware containing a radiation source was under consideration, such as a SNAP series of reactors, then the entry would be in the Preliminary Component Hazard Identification Series (Fig. 2), cataloged under 4.0 Low Energy Phenomena, 4.1.3 Radiation, with specific requirements entered under the Hazards Control column suitable for inclusion in specifications and/or procedures.

## B. Destructive Energy Related Forms (Fig. 7)

Example — Battery explosion caused by collection of hydrogen gas from battery operations.

Entries on the Form — The energy-related form contains an entry for classification of the hazard under consideration. In this case, the hazard was an exploding battery, and a battery is a high energy component. Thus, the classification will be entered as "3.0 High Energy Component." The next entry, "System/Subsystem/Component", is, obviously, "Batteries". For convenience as well as for future reference, the source of the information may be cited as well as the associated date.

The body of the form now requires an entry, first, in the left hand column the energy source should be cited. In our example, the energy source is clearly chemical, 3.3 in our indexing system. The next column is headed "Release/Transfer Mechanism". There are two situations that can release or transfer energy; either acts or conditions. "Acts" refer to two situations in which the human acts as the accident trigger through either deficient procedural controls or human error. "Conditions" refer to either an inherent design originated hazard or an error in manufacturing. In this example, an "act" is not applicable since the mere collection of hydrogen gas is not an act within the context of this classification system. The absence of a venting system leading to the collection of hydrogen gas was a design error, thus it is cataloged as a "condition". Consequently, within the second column under the subtitle of "conditions", an entry will be made citing the proximity of the ignition source and the energy source. If they were separated, an explosion would not occur. Completion of this entry will then complete the "Hazard Identification." The energy source has been identified as well as the triggering mechanism.

The third column, "Hazard Control", should contain an entry aimed at eliminating the identified hazard.

Four divisions of hazard controls have been identified in this system as described previously. In this example, control of the identified hazard requires venting of storage batteries to prevent collections of hydrogen gas, which is a design rather than a procedural requirement. Thus, the hazard control will be cited under "Configuration Design Criteria". This entry does not specify how batteries will be vented or the disposition of vented gases; that is, the engineering problem confronting the designers. The entry only states that venting will be required in appropriate specifications, and the checklist item only reminds safety engineers as well as design engineers and specification writers that batteries should be vented.



## C. Analysis of Functional Areas

The preceding two illustrations dealt with a specific phenomenon (atomic radiation) and with a specific component (batteries). These are limiting situations and find limited use, especially in early program phases when general concepts and broad guideline plans are of primary concern. Among the basic concerns of preliminary and advanced planners are the nature and scope of potential problems associated with the various schemes under consideration. Foremost among potential problems are, quite naturally, those concerning safety of the equipment as well as the safety of people. The energy-based technique can be structured to deal with these types of situations. The area of transportation has been selected to support this claim.

Example: Transportation Operations — Moving commodities from their point of origin to their point of utilization is vital to business success in both the private and the public sector of the economy. In the private sector it forms part of the distribution system intended to reach extensive markets with competitive products. Access to markets forms the basis for a free enterprise economy that is itself a marketing and distributing system. A method of transportation that delivers commodities inexpensively, safely, and swiftly to market is quite obviously a necessary and vital part of that system.

In the public sector emphasis is somewhat altered to the extent that the distribution system is restrictive. Excepting special cases, such as the military requiring continual resupply, the preponderance of distributions are on a "case-by-case" basis. Operations are carried out to satisfy requirements of a single or specific job following which they are discontinued. Additionally, costs are rather secondary, giving way to schedules and safety considerations. This is true since "deliverable value" is not a fiscal but a functional measure.

Both systems possess certain underlying similarities, however, which are based primarily on schedule considerations and on product safety. The commodity to be either economically rewarding or functionally useful must be delivered in useable condition — that is, safely. For this to be accomplished, it — the commodity — must be protected from damage arising from conditions encountered during movement.

For such protection to be effective, it is necessary to anticipate and guard against conditions that could prove damaging. That is, hazards to the commodity in the form of unsafe acts or unsafe conditions must be identified.

The broad and most obvious hazards are readily identifiable and, as such, are seldom experienced since protective measures negate their effects

upon the commodity. It is the unexpected and not quite so obvious hazard that escapes identification and results in damage to the commodity.

It is necessary, therefore, to afford protection to commodities from all hazards, the obvious as well as the not so obvious, during transportation operations and, to do that, comprehensive measures embodying methodical identification must be adopted. An array of complex and interacting conditions keyed to commodity characteristics and ranging from peculiarities in the mode of handling, of packaging, and of stowage practices and in procedures must be identified and diagnosed for hazardous considerations. Contributing factors must be assessed, and reasonable protective measures must be adopted to ensure damage free delivery. During initial planning, hazards identification relies principally on predictions of anticipated conditions and their effects. Forecasting probable future events of this nature suggests employment of subjective as well as comparative approaches to problem resolutions. The subjective approach relies on personal experience transferred from previous relevant jobs. All predictions recognize an element of subjective judgment, and personal skill must, therefore, play a part in the effort to identify hazards. However, hazard identification operations that are wholly subjective are of limited value since they are based on the recollections of which the individual involved has personal experience and, consequently, do not allow adequately for other experience which may be relevant. As is generally recognized, personal recollections are not entirely reliable.

Comparative methods are based on detailed records of previous experiences encountered in developments and may be used to make direct comparisons of past conditions with those anticipated, together with protective measures previously adopted. In virtually any proposed development a number of, in this case, transportation problems will correspond quite closely to problems encountered during previous developments. The similarity analysis of identified hazards is the citation of those actually experienced in the most similar circumstances (after allowing for some changes because of commodity differences, technology advances, etc.) and using this information as the estimate for hazards to be expected in the program under study. The records referred to are of a more practicable value when formulated as "checklists." However, "checklists" that are random and undisciplined are of little value to systematic study. Not only should checklists be compiled, maintained, and updated, but they should be organized in a consistent and meaningful manner to facilitate their use. Cataloging technique is one of the principal advantages of the energy-based system for hazard identification. Beyond organization of checklists, it is necessary to organize the area under study into manageable segments as restrictive as practicable to ensure careful consideration of all energy-based phenomena.

In the transportation area it may be useful to define transportation operations for the purpose of hazard identification in broad terms, inclusive of all potential influences upon the commodity. Transportation may be defined, therefore, as the movement of commodities or products from one geographical location to another, together with all supporting activities by four modes; air, railway, water, and roadway.

Refinement into more manageable segments may be approached through the use of a broad and simplified functional schematic of operations constituting transportation. Thus, the operation may be considered as consisting of: (1) loading the commodity on a carrier, (2) moving it to a destination, and (3) off-loading the commodity. Such a basic treatment implies a number of questions that immediately suggest its inadequacies. How is the product contained? Is it packaged? What equipment is used in loading, unloading, and stowage? What are the characteristics of the commodity? What type of carrier is used, and what route will it travel? Lastly it may be asked, by what process were the carrier, the route, the packaging, the handling equipment, and the stowage requirements determined? This last question suggests management involvement in decision making which in turn suggests technical involvement in problem solving.

It would not be too difficult to argue a planning function to plan and organize the activity, nor a design-engineering function to create the equipment required to carry out the activity, nor a manufacturing and testing function to produce the equipment and demonstrate its capability in satisfying requirements. All of these activities precede the act of movement. The functional schematic is not, therefore, representative of all influences upon commodity movement nor does it meet the intent of the definition cited above.

A more inclusive approach may possibly be found in identifying all activities, including managerial, technical, and operational, that constitute the process of moving commodities safely. These are planning, design engineering, manufacturing and testing, and operations and are the same generalized functions that attend any engineering development activity.

These generalizations may be adopted to transportation questions by identifying tasks that are to be performed. In planning (using the commodity and its characteristics as an input), the mode, route, cost, and schedule estimates are decided, and generalized instructions embodying those decisions are issued to design engineering. In arriving at those general decisions, hazards must be identified, trade-offs made, and safety considerations incorporated into the instructions issued to design engineering.

Adopting the energy-based concepts to hazard identification for transportation systems studies in this initial phase will be limited to those conditions expected to be met during functional activities (Fig. 8).

The mode itself suggests certain energy-based hazards arising from both carrier-systems-generated environments and from natural environments. Railway transport suggests system environments such as applied vibrations from road beds and high shock from humping during train makeup at railway yards.

In regard to natural environments, routes through areas adjacent to and in sea atmospheres suggest salty atmospheric environments that may lead to corrosion problems. Destination may even induce effects that threaten or damage commodities. The Air Force, for example, air transported a missile in a sealed container from its manufacturing site, geographically located at a high elevation, to a base located at a lower elevation. The package was opened and when the missile was withdrawn from the container, its tanks collapsed. The collapse was the result of the pressure differential, the low pressure of the manufacturing site coupled with the high ambient pressure at the delivery site, acting upon the tanks.

Planning apparently failed to take into account the varying hazards attendant to widespread military usage when developing general requirements governing transportation operations. In this instance the energy source overlooked was that arising from high energy natural environments, specifically those posed by atmospheric pressure. The hazards experienced during shipment were apparently provisioned since the packaged missile was delivered undamaged, and if it had been opened at an elevation comparable to that of the manufacturing site, no damage would have occurred. It is interesting to speculate that if a comprehensive hazard identification procedure had been available, would this particular hazard have been recognized and avoided? Here we are quite obviously engaging in problematical speculation, but the odds tend to favor hazard identification and avoidance when a methodical and comprehensive identification procedure is used.

In the context of the energy-based identification system discussed in this document, it may be of interest to answer the question identifying the energy release mechanism. In this case, the mechanism was a "condition" triggered by exposure to a high energy source (ambient atmospheric pressure). The pressure differential thus created by the container design (low internal tank pressure — high external atmospheric pressure) crushed the tanks. In a more objective manner, it may be described as the outside pressure pushing

		ACTIVITY	PLANNING		DESIGN ENGINEERING			MFG/TESTING	OPERATIONS						
			MODE	ROUTE	PACKAGE CONTAINER REQTS	STORAGE REQTS	HANDLING REQTS	CARRIER REQTS		PACKAGING	HANDLING	STORAGE	TRANSPORTING	OFF LOADING	PACKAGE REMOVAL
CRITICAL ENERGY NEEDS	PHYSICAL	WARNING/ABORT/ESCAPE													
		SYSTEM CONTROL													
		INFORMATION/REQUIREMENT													
		INTERFACE CAPABILITY													
		HUMAN ERROR/FAILURE													
	PHYSIOLOGICAL	HUMAN CAPABILITY													
HIGH ENERGY ENVIRONMENTS	SYSTEM GENERATED ENVIRONMENTS	DYNAMIC LOADS													
		ACCELERATION													
		VIBRATIONS													
		ACCOUSTICAL													
		PRESSURE/VACUUM													
		STATIC LOADS													
		SHEAR													
		TENSION													
		COMPRESSION													
		THERMAL													
NATURAL ENVIRONMENTS	ELECTRICAL/ELECTRONIC														
	LIGHTNING														
	WIND														
	RAIN														
	PROJECTILES														
	TEMPERATURE														
	EARTHQUAKE														
	SALT SPRAY														
	PRESSURE/VACUUM														
HIGH ENERGY CONDITIONS	BASIC ENERGIES	POTENTIAL													
		KINETIC													
		CHEMICAL													
		NUCLEAR													
	TOXICANTS	INHALANTS													
		INGESTA													
		RADIATION													
		ABSORPTION													
		CORROSION													
		EMBRITTLMENT													
PHYSICAL CONTAMINATION	AGING														
	SURFACES														
	ORIFICES														
	FILTERS														

Figure 8. Hazard identification planning chart – transportation.

against the lower internal pressure of the tank until an equilibrium point was reached in which the differential across the tank walls was zero. In the process of reaching equilibrium the metal walls were distorted to the point that they were no longer useable.

This example illustrates two very important aspects of hazard identification: (1) the need for a methodical and comprehensive identification procedure, and (2) its use early enough to have a decided influence upon planning and design engineering.

In its application to the transportation problem, an energy-based approach recognizes that each mode available for use presents various forms and magnitudes of energies acting upon the carrier-commodity as a unit as well as upon the commodity itself. These forms and magnitudes of energies generally arise from conditions imposed by the medium in which the carrier moves. For example, conditions in air and water are quite different from those encountered on roadways. The effects of conditions are implicit throughout the system influencing carrier design, package design, handling techniques, and stowage techniques. It may be argued that these conditions primarily affect the carrier and have only a secondary effect upon the commodity. This is true to the extent that the commodity has been shielded from those effects as recipients of broken merchandise are aware. In arriving at a definition of those provisions necessary to shield the merchandise from damage, the conditions to which the package is subjected throughout its movement including the effects transmitted by the carrier must be identified and protective precautions must be taken. In addition, conditions acting independently upon the commodity must be identified and their damage potential assessed. These may include such conditions as high or low temperatures, humidity, salty or corrosive atmospheres, pressures, etc. A large number of the conditions that pose threats can be identified during planning studies merely by considering the mode and route proposed in light of the characteristics of the commodity. High pressure differentials will always pose threats to thin wall tanks, high vibrations and shocks to fragile material, salty atmospheres to untreated metal surfaces, and low temperatures to elastomeric materials. The problem is compounded, but by no means insoluble, when qualitative relationships of combined environments are studied for hazard potentials (Fig. 9).

Incorporation of the information, identifying hazards to be expected into the general requirements issued by planning to design engineering, is of considerable use in developing realistic specifications, drawings, and procedures for transportation equipment. In our example, if the hazard arising from pressure differentials had been cited in the general requirements issued by



should concern itself with the adequacy of protection afforded the commodity from hazards identified during planning activity, providing requirements for incorporation in specifications and procedures, and reviewing designs to identify specific hazards introduced by specific designs. The procedure used during planning, that is, identifying the energy source and identifying the release mechanism, readily adopts itself to safety studies conducted during this period.

Manufacturing is the function that translates designs and specifications into tangible products, containers, shock and vibration mounts, protective closures, and handling equipment used in transporting the commodity. Safety operations should ensure that approved specifications and drawings are faithfully executed. Quite frequently design changes are necessitated by manufacturing considerations and it is important that such changes do not introduce new or additional hazards. Also, it is important that such changes as are introduced are reviewed and that such changes as are adopted are adequately treated in procedural documents.

Testing may or may not be performed to establish design and manufacturing acceptability of the final product. In so far as transportation equipment itself is concerned, testing demonstrates for the designer as well as for safety engineering that specifications are met. Additionally, safety can verify such things as location and need for handholds, handling equipment attach points, clearances, center of gravity locations, and also check such activity as covered in procedural documents to establish their completeness in using the equipment. A careful investigation of tangible hardware is usually a profitable exercise in hazard identification, and it is surprising just how many real or potential hazards overlooked during drawing reviews are discovered by actually looking at the finished product. This type of activity may also be carried out during reviews conducted at the manufacturing location.

Operations designate the period during which the commodity is packaged, handled, stowed aboard a carrier, transported, off loaded, and the package removed. The activity is governed by procedural documents that should include provisions for avoiding known hazards. Many hazards to the commodity that were identified as predictive precautions incorporated into design specifications and procedural documents can be verified by auditing actual conditions. During these audits many additional hazards that escaped notice may come to light. In the example cited previously of air transporting a missile, an audit aimed at checking off all energy sources actually encountered would in all probability have identified atmospheric pressure differentials. In the event one-of-a-kind or an extremely valuable commodity is transported, a dry run of actual operations may aid appreciably to energy source and release mechanisms identification.



To the list of activities making up "operations," package removal has been added, since in many instance commodities are damaged during this operation.

It is during actual movement that the commodity is most vulnerable to damage from totally unexpected sources. For example, in the first overland transit of an Atlas missile from San Diego to Patrick Air Force Base, the missile arrived full of bullet holes. No one could have foreseen the threat posed by irresponsible marksmen along the route. It is for this reason, to minimize unexpected damage, that past histories of movements similar to the one contemplated should be reviewed and the previous experience used during hazard identification activities.

The preponderance of hazards arising from transportation activities used thus far as illustrations have been those whose basic energies are bound up in high energy environments. Given the diversity of these activities, however, there are hazards that threaten the commodity whose basic energy sources originate in high energy components and low energy phenomena as well as in the area of critical energy needs.

During the "operations" phase, handling activities are performed that involve simply picking up the packaged or unpackaged commodity. Any time the commodity is raised, either by hand or by the use of specialized handling equipment (forklift trucks, cranes, derricks, etc.), potential energy is imparted to it. If the commodity is dropped the potential energy is released and will, unless the packaging is specifically designed to neutralize and absorb the resulting foot-pounds of energy, inflict damage upon the commodity. In those cases where unpackaged commodities are handled, potential energy is a very serious source of potentially damaging energy that can be released by a number of mechanisms arising from either acts of personnel or conditions of the equipment or commodity. Improperly trained personnel operating the handling equipment can, through a control or operating error, cause the commodity to either strike the ground or strike an obstruction. Personnel can improperly secure the commodity to the handling equipment, especially in the absence of specially designed attach points, causing it to slip from the restraints, which in itself may impart sufficient shock loads to cause damage or a fall to the ground. In moving by overhead crane or by forklift truck, the commodity not only possesses potential energy by virtue of its elevation but also kinetic energy imparted by the moving carrier. On one occasion a forklift truck loaded with a "lift" of 24 gage galvanized sheet steel was proceeding down an aisle in a storage area when a female employee, walking down an intersecting aisle, appeared suddenly in front of the moving truck. The

operator panicked and jammed on his brakes, releasing the kinetic as well as the potential energy of the sheet steel. The end result was that the female's heel was severed with almost surgical perfection. In this case an "act" was the primary release mechanism, that of the operator's immediate application of the vehicle's brakes. A condition also acted as a release mechanism, even though it was of a secondary nature. The condition was the absence of "banding" to secure the "lift" of steel together as a unit. If banding had been used, the inertia would have been enough to have released only the potential energy and the material would have only fallen to the floor in front of the truck, not reaching the victim at all. This condition coupled with the characteristics of the commodity, a very slick surface with an extremely low coefficient of friction, very thin material, and wide flat sheets which contributed a dynamic lifting factor, thus served to extend the range of the moving sheets and ensure the subsequent events. In this case, damage was inflicted by the commodity, not to the commodity, for the sheets were later cleaned, restacked, and shipped to the customer.

There are situations where the carrier is subjected to severe buffeting by the medium through which it travels, and the carrier imparts applied loads to the stowed commodity; when the stowed commodity is properly battened, it will move with the carrier but if it is improperly stowed and battened, it will in all likelihood shift. The commodity may possess characteristics that will destroy the carrier itself as well as inflict damage on itself; for example, in cases of kinetic energy being released and damage inflicted when the commodity strikes an obstruction.

In the case of the release of chemical energy, the most graphic examples lie in transporting chemicals, especially volatile chemicals. Ammonium nitrate is a fertilizer; however, a ship containing this commodity was involved in a very well known explosion in a Texas port some years ago which inflicted catastrophic damage when the chemical energy was released. Transportation of such chemicals as liquid oxygen, liquid hydrogen, red fuming nitric acid, natural gas, reactive hydrocarbons, and the like all possess basic chemical energy that may be released by either "acts" or "conditions" or a combination of both. In situations of this nature, not only is the commodity as well as the carrier generally lost but damage is inflicted on surroundings and may directly cause loss of life or property damage.

The carrier itself may possess chemical energy by virtue of its operational characteristics in the form, for example, of gasoline, oil and/or grease. Leaking gasoline through loose fuel line connections or gas tank ruptures could cause the carrier to burn, destroying itself as well as the commodity. Thus,

the safety of the carrier has a direct bearing upon the safety of the commodity during transportation. Wooden truck bodies covered with canvas have served as tinder for an ignition source with loss of expensive and one-of-a-kind commodities in the ensuing fire. If, for example, an all-metal truck body replaced the wood-canvas models, a fire might be averted even though the same ignition source is present, since the tinder, the fuel (wood and cotton fabric), would not be present. In terms of the energy-based doctrine, the energy source has been isolated from the energy release mechanism.

At first glance the area of critical energy needs appears moot when considering hazards in transportation. Careful thought will soon convince an observant analyst that this area is definitely applicable, not only for critical physical energy needs of the carrier in the form of steering and braking functions but also for the preservation of certain perishable or fragile commodities. Any commodity that requires controlled conditions to ensure its safe delivery imposes energy needs to meet those controlled conditions. Refrigeration for certain produce, dairy products, meats, etc., must be supplied and is critical to the safety of the commodity. The current energy crisis is demonstrative of this situation as when stranded long-haul carriers of produce lost their cargos from spoilage when refrigeration systems had to be shut down. Transportation of liquid oxygen and hydrogen imposes a heat shielding requirement to ensure the very survival of the commodity. The necessity for maintaining controlled environments implies the need for information and command to ensure that conditions are maintained and to command environmental equipment to perform its expected function. It was the need of controlled conditions that led the Air Force to design containers for its missile which completely isolated the missile from its surroundings while in transit from its Denver manufacturing site.

Low energy phenomena also contribute to hazards adversely affecting commodities during transportation. Physical deterioration by corrosion can be induced by environmental conditions, as mentioned previously. Physical contamination can easily be induced by dust particles in the air or by dirty carriers on unprotected or poorly packaged commodities. Frozen foods that may thaw during movement and then be refrozen may suffer bacterial growth during that period which could later poison the ultimate consumer. Thus, while the commodity is not physically contaminated, it is chemically contaminated and becomes essentially a toxicant.

This brief review should serve to illustrate that all of the four classes of hazardous energies are present to a greater or less degree in transportation

activities, identified by the characteristics of the commodity itself, the carrier, and the mode selected. To ensure thoroughness, however, it has been suggested that the energy-based method be used for studies or investigations in each program phase, identifying first the energy source (Table 1) and second, the release mechanism. Additionally, it has been suggested that previous transportation activity be analyzed for the purpose of developing "disciplined" checklists which record not only the identified hazard, but also the measures initiated for its elimination or control (Figs. 6 and 7).

## BIBLIOGRAPHY

Following is a list of selected speeches and publications by Dr. Leslie W. Ball:

1. Contracting for Safety. Presented to the NASA Government/Industry Systems Safety Conference at the Goddard Space Flight Center, Greenbelt, Maryland, May 26, 1971.
2. Cost Reduction by Integration of the Assurance Technologies. Presented to the AIAA Conference on "Man's Role in Space" at Cocoa Beach, Florida, March 28, 1972.
3. Hazard Control Through Designer Education. Taped presentation to the "Institute for Accident Prevention" symposium in Cologne, Germany, April 24, 1972.
4. Integration of Safety Engineering Into a Cost Optimized Development Program. Presented to SAWE (Society of Aeronautical Weight Engineers) in Atlanta, Georgia, May 22, 1972.
5. Safety Achievement Through System Engineering. Presented at the Southern Area Research and Development Safety Symposium at the University of Tennessee Space Institute, Tullahoma, Tennessee, May 7-8, 1973.
6. Safety Inputs to Development Program Plans. Presented to the Tenth National Reliability and Maintainability Conference at Anaheim, California, June 28, 1971.

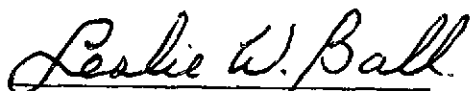
## APPROVAL

### RECORDING AND CATALOGING HAZARDS INFORMATION

By Richard J. Stein

The information in this report has been reviewed for security classification. Review of any information concerning Department of Defense or Atomic Energy Commission programs has been made by the MSFC Security Classification Officer. This report, in its entirety, has been determined to be unclassified.

This document has also been reviewed and approved for technical accuracy.



LESLIE W. BALL

Director, Safety and Manned  
Flight Awareness Office