UNCLASSIFIED

AD NUMBER
AD862338
LIMITATION CHANGES
TO: **Approved for public release; distribution is unlimited.**
FROM: **Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use; 28 NOV 1969. Other requests shall be referred to Government-Industry Data Exchange Program, Washington, DC.**
AUTHORITY
GIDEP/Seattle Services Div. ltr dtd 23 Jan 1974

THIS PAGE IS UNCLASSIFIED

AD862338

BOEING

CODE IDENT. NO. 81205

NUMBER D2-113072-1

TITLE: System Safety Analytical Technology - Preliminary Hazard Analysis

AD No.
DDC FILE COPY

see form 1473

DDC
RECEIVED
DEC 15 1969
C

STATEMENT #3 UNCLASSIFIED

Each transmittal of this document outside the agencies of the U.S. Government must have prior approval of The Boeing Company Seattle, Washington 98124

SEATTLE, WASHINGTON

Best
Available
Copy

STAT[illegible] 1

[illegible] of the
U.S. Government must [illegible]

REV LTR

THE BOEING COMPANY
Aerospace Group
Seattle, Washington 98124

CODE IDENT. NO. 81205

NUMBER D2-113072-1

TITLE: System Safety Analytical Technology -
Preliminary Hazard Analysis

ORIGINAL RELEASE DATE _____. FOR THE RELEASE DATE OF SUBSEQUENT REVISIONS, SEE THE REVISIONS SHEET. FOR LIMITATIONS IMPOSED ON THE DISTRIBUTION AND USE OF INFORMATION CONTAINED IN THIS DOCUMENT, SEE THE LIMITATIONS SHEET.

MODEL All ASG

ISSUE NO. _____

ISSUE TO _____

PREPARED UNDER:

☐ CONTRACT NO.

☒ IR&D

☐ OTHER

PREPARED BY C. A. Ericson 12-1-69
C. A. Ericson

SUPERVISED BY H. D. Trettin 12-1-69
H. D. Trettin

APPROVED BY H. F. Eppenstein 12-1-69
H. F. Eppenstein

APPROVED BY H. D. Trettin 12-1-69
H. D. Trettin

Edited by C. R. James 11/24/69
C. R. James

12-[illegible]

U3 4802 1433 REV. 9 68

SHEET
1

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS				SHEET NUMBER	REV LTR	ADDED SHEETS			
		SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR			SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											

REVISIONS

LTR	DESCRIPTION	DATE	APPROVED

3-4672-1(1), SHEET 4/44

LIMITATIONS

All U. S. Government agencies may obtain copies directly from DDC. The DDC is requested to route all other requests to Boeing for approval.

This document is controlled by Reliability, System Safety and Value Engineering

All revisions to this document shall be approved by the above noted organization prior to release.

Abstract and Key Words

This document describes the method for performing a Preliminary Hazard Analysis (also known as a Gross Hazard Analysis) and using the derived results. This analysis is a method for identifying hazardous elements, hazardous conditions, and potential accidents; determining the significance of their potential effect; and establishing initial design and procedural safety requirements to eliminate or control these identified hazardous conditions and potential accidents. The data and information thereby derived can be used to serve other initial system safety needs, such as prediction, planning, and priority allocation.

System safety
Hazardous element
Hazardous condition
Accident - Potential
Accident prevention measures
Safety analysis

USE FOR TYPEWRITTEN MATERIAL ONLY

U 9 4002 7494 REV. 8-69

TABLE OF CONTENTS

		Page
1.0	PURPOSE	7
2.0	RESULTS	9
3.0	METHODOLOGY	10
3.1	Basic Approach	10
3.2	Approach	11
3.3	Hazardous Element Checklists	12
3.4	Technique	17
3.5	When Performed	20
3.6	Data Required	21
4.0	EXAMPLE	22
5.0	REFERENCES	26

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4002 1434 REV. 8-65

1.0 PURPOSE

The Preliminary Hazard Analysis (PHA) is a method of system/subsystem/function analysis, developed and used by system safety engineering. The primary purposes of this analysis technique are to:

1) identify hazardous elements, hazardous conditions, and potential accidents
2) determine the significance of their potential effect
3) establish initial design and procedural safety requirements to eliminate or control these identified hazardous conditions and potential accidents.

In addition, the data and information derived from this analysis will serve other initial system safety needs, such as:

1) foresee hardware, procedural, and system interface problem areas
2) provide information that will assist in planning a safety program
3) provide visibility to management for safety program manloading and costing
4) establish priority for safety effort scheduling
5) identify areas for testing
6) identify areas for further analysis, particularly undesired events for fault tree analysis.

The PHA should be performed as early in the product program as possible, preferably during the conceptual stage, with scheduled updates as design development progresses. This provides the basis for the establishment of design safety requirements early in the program: thus, ideally, eliminating the possibility of design changes later in the program, which would be very costly.

The PHA can be initiated during any stage of product development with satisfactory usefulness. If the safety program commences at the conceptual phase of product development, initial safety requirements can be established from the PHA. If the safety program commences at some other stage of product development (i.e., Manufacturing), initial safety requirements cannot be established, and possible design changes may be imminent. However, whenever the safety program commences, the first analysis conducted should be a PHA. This is because, in identifying safety critical areas, the PHA also provides necessary information for planning and implementing the ensuing safety program.

In establishing initial safety requirements, the PHA is a means of investigating related program experience to determine what pitfalls have already been experienced in similar designs and what controls have been found necessary.

USE FOR TYPEWRITTEN MATERIAL ONLY

U9 4002 7494 REV.8-65

The name given to the PHA is somewhat misleading. Since the PHA is usually always the first safety analysis performed in a system safety program (or at least it should be), it has thus derived its name from being the Initial or "preliminary" analysis. However, as the PHA is updated during the program, it still retains the "preliminary" in its name. Therefore, the information contained in the PHA should not be thought of as being preliminary in nature, but as broad and not detailed.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4002 7494 REV. 8-65

2.0 RESULTS

The results of the PHA are the documentation of the recognized and anticipated design safety pitfalls and the method by which these pitfalls are to be avoided. The methods of avoiding such pitfalls generally include:

1) establishing preventive measures
   a) Initial safety requirements - design, procedural, personnel
   b) safety devices
   c) design changes

2) identifying areas requiring further investigation
   a) areas for further safety analysis and type of analysis
   b) areas requiring testing
   c) areas requiring trade studies

3) identifying applicable documents and standards.

In establishing requirements as preventive measures, the work does not always need to be original. In many areas of safety concern, design safety data already exists. This data is contained in applicable documents in the form of standards, criteria, specifications, requirements, and guidelines. Safety design data documents should be researched by the safety engineer, all applicable documents should be identified, and applicable safety portions specified, so that the designer knows exactly what is required. All applicable documents must be specified in order to avoid guess work with regard to what documents are applicable. If a mission requirement prevents the use of established safety design data, the PHA should reveal why they can't be used and show what design data will be applied to accomplish the intent of the established design data, or what customer waivers will be necessary.

The results of the PHA are used by both design and system safety engineering. Design engineering uses the results in their decision making process, to ensure an optimum safe design. In some respects the safety requirements serve as guidelines and/or constraints, from within which the designer must operate. Safety engineering uses the results as a safety baseline, from which the safety of future designs can be compared. In addition, the results provide a "road map" for follow-on safety studies, analyses, and testing.

USE FOR TYPEWRITTEN MATERIAL ONLY

U9 4007 7494 REV. 8-65

3.0 METHODOLOGY

3.1 Basic Approach

The particular approach used in the accomplishment of the PHA is dependent upon such variables as funding, available time, and product sophistication. The documentary format of each approach is, in itself, a method of performing the analysis. To date, three acceptable approaches, and their related formats, are in existence. Commonly, they can be identified as:

1) columnar form with specific entries
2) top level fault tree
3) narrative description.

Although these approaches differ considerably, the basic content of their formats is very similar. That is, each approach results in the identification of hazardous conditions and potential accidents, with their related probable causes and potential effects. Primarily, the major difference between these approaches is the rigor of the method, the amount of information generated, and the overall usefulness of the information generated by the analysis.

The PHA approach utilizing the columnar form, with specific detailed entries in each column, appears to provide the optimum results for most programs. This format establishes a means for systematically searching and recording specific hazard information with regard to systems, and storing this information so that it is easily retrievable and usable. It is a cost effective approach, in that it is not time consuming to perform. This method is particularly desirable because it provides superior program visibility, in addition to fulfilling the primary purpose of the PHA.

A top level fault tree, following the mechanics of fault tree analysis, fulfills the primary objective of a PHA. Although this analysis approach provides a systematic method of identifying hazardous conditions and potential accidents, it applies itself more readily to identifying the causes of these undesired events. Structuring the top level of a fault tree is generally the most difficult and time consuming phase of a fault tree analysis. Furthermore, although the fault tree is developed by graphically analyzing undesired events, it is sometimes difficult to specifically identify a particular event as a hazardous condition, a hazardous element, or a potential accident.

The narrative approach to the PHA is less rigorous, and usually less complete than the other two approaches, because to be equally detailed in a narrative writing style is a lengthy and backbreaking task. This approach is less susceptible to systematic method or technique, and, therefore, the results usually have serious gaps or incomplete areas. The hazardous conditions and potential accidents are

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4007 1494 REV. 8-67

generally identified from experience, and then are explained in great depth and detail, more on the order of a final report than an analysis.

3.2 Approach

Using the columnar format, a PHA is initiated by dividing the system into convenient working sections, a working section being a subsystem, function, or any other logical system element which is small and easy to work. Each working section is investigated individually, and all hazardous elements existing in or associated with the design of that working section are identified. Then a determination is qualitatively made as to what is "risked" (i.e., personnel, hardware, mission) due to the hazardous element being present in the system. Needless to say, the item must be of appreciable "value" in order for it to sustain a risk or be in jeopardy. By determining how the hazardous element causes the risk to the item of value, the hazardous condition is indirectly identified. For example, hydrazine places a risk upon personnel during handling operations. The risk to the personnel could be due to toxic vapors. Therefore, a potential accident is established as "exposure of personnel to toxic vapors" and the associated hazardous condition is then identified as "unconfined hydrazine in the presence of personnel."

Now, the logical question is how to determine the hazardous elements. A hazardous element is any item or function which, when in a system environment, constitutes a threat or jeopardizes something of value, within or related to that system. The item or function may be inherently hazardous by itself, such as radioactive material, or it may be hazardous only when in combination with other items and/or functions, such as heat producing components. The key idea behind a hazardous element is that some value is being risked by having that element present in the system. Essentially, there are four methods for identifying hazardous elements: 1) through the use of checklists, 2) from experience, 3) engineering judgment, and 4) intuition.

Hazardous elements can be recognized through checklists by comparing the hardware elements or functions contained in the system design against the known hazardous elements on the checklist. There are many different checklists existing, as the following examples indicate:

1) general hazardous element sources (Figure 3-1)
2) hazardous energy sources (Figure 3-2)
3) hazardous acquisition functions (Figure 3-3)
4) hazardous mission functions (Figure 3-4)

Hardware elements or functions which correlate with items on a checklist indicate a safety critical area or a hazardous element. However, such a checklist is more than just a list with which to check off the system design, it is a list which is intended to stimulate ideas as to how or where an unrealized hazardous element could exist.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 2002 1494 REV. 6-69

Experience from related programs provides information for identifying hazardous elements and safety critical areas. Previous safety problem areas encountered on similar hardware elements or functions which are presently being considered will indicate areas requiring special attention. The major problem here is that safety data retention centers are still maturing and all needed information may not be readily accessible. When such is the case, further identification of hazardous elements, not already encountered by way of checklists or experience, is accomplished through engineering judgment and/or intuition.

3.3 Hazardous Element Checklists

Since no single checklist is ever really adequate in itself, it becomes necessary to develop and utilize several checklists. Even though this will result in some repetition, complete coverage of hazardous elements will be more certain. Special checklists should be developed for the specialized needs of different programs, such as space programs, missile programs, aircraft programs, marine programs, etc. With the invention and usage of new hardware elements and functions, new hazardous elements will develop, requiring expanded and updated checklists.

The following are typical checklists used in recognizing hazardous elements and safety critical areas. These checklists, which are examples and are not intended to represent ultimate checklist sources, are as follows:

Figure 3-1 is a list of general sources which have been found to produce hazardous conditions and potential accidents, when the proper system conditions are present. This list should stimulate ideas as to where possible hazardous elements could exist in any particular system.

Figure 3-2 is a list of energy sources which are considered to be in themselves hazardous elements when used in a system environment. This is due to the potential effects from an energy source, should it be released within the system.

Figure 3-3 is a list of functions which are hazardous due to the materials used or to the critical nature of the operation. This list generally applies to programs in the acquisition phase, which includes manufacture, test, handling, transportation, and installation.

Figure 3-4 is a list of functions which are hazardous due to the materials used or to the critical nature of the mission. This list is an example particularly intended for space programs.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4602 1494 REV.8-65

1. Acceleration
2. Contamination
3. Corrosion
4. Chemical dissociation
5. Electrical
   - shock
   - thermal
   - inadvertent activation
   - power source failure
   - electromagnetic radiation
6. Explosion
7. Fire
8. Heat and temperature
   - high temp
   - low temp
   - temp. variations
9. Leakage
10. Moisture
    - high humidity
    - low humidity
11. Oxidation
12. Pressure
    - high
    - low
    - rapid changes
13. Radiation
    - thermal
    - electromagnetic
    - ionizing
    - ultraviolet
14. Chemical replacement
15. Shock (mechanical)
16. Stress concentrations
17. Stress reversals
18. Structural damage or failure
19. Toxicity
20. Vibration and noise
21. Weather and environment

Figure 3-1 Checklist of General Hazardous Element Sources

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4802 1434 REV. 8-65

1. Fuels
2. Propellants
3. Initiators
4. Explosive charges
5. Charged electrical capacitors
6. Storage batteries
7. Static electrical charges
8. Pressure containers
9. Spring-loaded devices
10. Suspension systems
11. Gas generators
12. Electrical generators
13. R. F. energy sources
14. Radioactive energy sources
15. Falling objects
16. Catapulted objects
17. Heating devices
18. Pumps, blowers, fans
19. Rotating machinery
20. Actuating devices
21. Nuclear

Figure 3-2 Checklist of Hazardous Energy Sources

USE FOR TYPEWRITTEN MATERIAL ONLY

U2 4802 1434 REV. 8-65

1. Welding
2. Cleaning
3. Extreme temperature operations
4. Extreme weight operations
5. Hoisting, handling, and assembly operations
6. Test chamber operations
7. Proof test of major components/subsystems/systems
8. Propellant loading/transfer/handling
9. High energy pressurization/hydrostatic-pneumostatic testing
10. Nuclear component handling/checkout
11. Ordnance installation/checkout/test
12. Tank entry/confined space entry
13. Transport and handling of end item
14. Manned vehicle tests
15. Static firing
16. Systems operational validations

Figure 3-3 Checklist of Hazardous Acquisition Functions

USE FOR TYPEWRITTEN MATERIAL ONLY

US 4802 1434 REV. 8-65

1. Crew egress/ingress
2. Ground to stage power transfer
3. Launch escape
4. Stage firing and separation
5. Ground control communication transfer
6. Rendezvous and docking
7. Ground control of crew
8. Ground data communication to crew
9. Extra vehicular activity
10. In-flight tests by crew
11. In-flight emergencies involving loss of communications, loss of power/control, fire toxicity, explosion, or life support system
12. Re-entry
13. Parachute deployment and descent
14. Crew recovery
15. Vehicle safing and recovery
16. Vehicle inerting and decontamination
17. Payload mating
18. Fairing separation
19. Orbital injection
20. Solar panel deployment
21. Orbit positioning
22. Orbit correction
23. Data acquisition
24. Mid-course correction
25. Star acquisition (navigation)
26. On-orbit performance
27. Retro-thrust

Figure 3-4 Checklist of Hazardous Mission Functions

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4802 1434 REV. 8-64

3.4 Technique

The recommended columnar PHA format is shown in Figure 3-5. This particular format has proven to be useful and effective in applied situations. As shown, this format provides for entries identifying hazardous elements and conditions, resulting potential accidents and their causes and effects, accident prevention measures to correct the situation, and design engineering feedback.

The following instructions are descriptive of the information required under each column entry of the form:

1) Subsystem or Function - This column identifies the hardware or functional element being analyzed.

2) Mode - This column identifies the system phases or modes of operation which are applicable.

3) Hazardous Element - This column identifies the elements, in the hardware or function being analyzed, which are inherently hazardous.

4) Event Causing Hazardous Condition - This column identifies conditions, undesired events, or faults which could cause (or trigger) the hazardous element to become the identified hazardous condition.

5) Hazardous Condition - This column identifies the hazardous conditions which could result from the interaction of the system and each hazardous element in the system.

6) Event Causing Potential Accident - This column identifies undesired events, or faults which could cause (trigger) the hazardous condition into becoming the identified potential accident.

7) Potential Accident - This column identifies any potential accidents which could result from the identified hazardous conditions.

8) Effect - This column identifies the possible effects of the potential accident, should it occur.

9) Hazard Classification - This column provides a qualitative measure of significance for the potential effect of each identified hazardous condition, according to the following criteria:

Class I - SAFE - Condition(s) such that personnel error, deficiency/inadequacy of design, or malfunction will not result in major degradation and will not produce equipment damage or personnel injury.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4807 1434 REV. 8-65

1 SUBSYSTEM OR FUNCTION	2 MODE	3 HAZARDOUS ELEMENT	4 EVENT CAUSING HAZARDOUS CONDITION	5 HAZARDOUS CONDITION	6 EVENT CAUSING POTENTIAL ACCIDENT	7 POTENTIAL ACCIDENT	8 EFFECT	9 HAZ. CLASS	10 ACCIDENT PREVENTION MEASURES			11 VALI-DATION
									10A1 HARDWARE	10A2 PROCEDURES	10A3 PERSONNEL	

REV LTR _____

MATRIX--PRELIMINARY HAZARD ANALYSIS

Figure 3-5

Class II - MARGINAL - Condition(s) such that personnel error, deficiency/inadequacy of design, or malfunction will degrade performance, but which can be counteracted or controlled without major damage or any injury to personnel.

Class III - CRITICAL - Condition(s) such that personnel error, deficiency/inadequacy of design, or malfunction will degrade performance, injure personnel, damage equipment or will result in a hazard requiring immediate corrective action for personnel or equipment survival.

Class IV - CATASTROPHIC - Condition(s) such that personnel error, deficiency/inadequacy of design, or malfunction will severely degrade performance and cause subsequent equipment loss and/or death or multiple injuries to personnel.

10) Accident Prevention Measures - This column is for establishing recommended preventive measures to eliminate or control identified hazardous conditions and/or potential accidents. Preventive measures to be recommended should fall into the following categories:

hardware design requirements
incorporation of safety devices
hardware design changes
special procedures
personnel requirements

11) Validation - This column is provided to record validated preventive measures and keep cognizant of the status of the remaining recommended preventive measures. This column should be completed by answering two questions: 1) has the recommended solution been incorporated, and 2) is the solution effective?

In filling out the columnar PHA form, the dynamic relationship between the entries should be kept in mind. This relationship is depicted in Figure 3-6. The hazardous element (i.e., propellant) must be acted upon or influenced by some (discrete) event or condition (i.e., static electricity) in order for it to become a hazardous condition. Then, when the hazardous condition exists, it must be acted upon by some event or condition in order for it to result in the potential accident. In addition to an event or condition, duration may be a factor in causing the hazardous condition to result in the potential accident. That is, in certain cases, if the hazardous condition is allowed to exist without immediate corrective action, it may result in the potential accident without any other event acting upon it.

USE FOR TYPEWRITTEN MATERIAL ONLY

NS 4802 1494 REV. 8-65

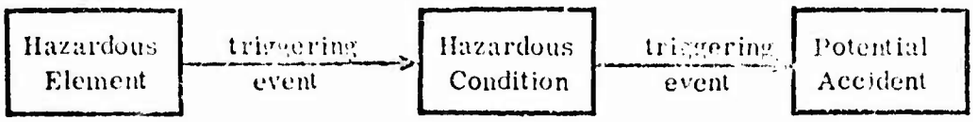

Figure 3-6 Relationship of Events Leading to an Accident

It should be noted that the information to go on the columnar form may not always be clear-cut or readily obvious. It is likely that, in some cases, special exceptions and deviations will be necessary. In some instances it will be found that the "cause event of the hazardous condition" is the same as the "cause event of the potential accident," except that the former is passive (a threat), whereas the latter is active (the threat being carried out).

3.5 When Performed

The PHA is generally started during the conceptual stage of program development. Then, as design development progresses, the PHA is iteratively updated in order that necessary safety design requirements can be established prior to each phase of more detailed design development.

Figure 3-7 shows a breakdown of the life cycle of a system and the corresponding PHA time relationship. As indicated, the initial PHA is performed during concept formulation. The PHA is then iteratively updated during contract definition and engineering development. It must be noted that this represents an ideal safety program, and that, in reality, strategic adjustments must always be made to suit the real-life requirements of the program.

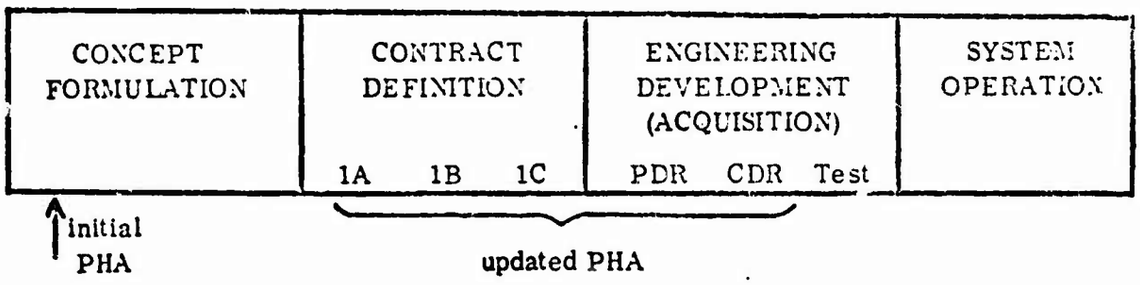

Figure 3-7 System Life Cycle

USE FOR TYPEWRITTEN MATERIAL ONLY

US 4002 1434 REV. 8-63

3.6 Data Required

As is the case with most analyses, the PHA is performed by utilizing whatever data is available. At the conceptual phase, the following data is essential. customer requirements and specifications (when an RFP is available), conceptual drawings, block diagrams, conceptual procedures, and conceptual trade studies. As design development progresses, more detailed data is used as it becomes available.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4802 1434 REV. 8-65

4.0 EXAMPLE

Figure 4-1 presents a partial example of a PHA performed on a missile subsystem. One example of a hazardous element in the missile has been identified as an ordnance device. More appropriately, the hazardous element in this case is the ordnance explosive(s) in the device. The system modes affected by this hazardous element have been identified as: transportation, handling, storage, installation, test, and operation.

Values endangered by including this hazardous element in the system environment are: personnel, property, and/or the mission. The potential accident that risks these items of value is the "inadvertent ignition" of the hazardous element - ordnance explosive(s). Thus, the hazardous condition is established as "explosives exposed to an ignition environment." That is, the hazardous element - explosives - is placed in an environment where it is highly susceptible to premature or inadvertent ignition. The undesired triggering events which could cause the existence of the hazardous condition to become the potential accident are then shown to include: premature signals, erroneous commands, RFI, EMP, EMI, excessive temperature, shock, and electrical misconnection. In this instance, neither the hazardous element nor the ignition environment can be eliminated from the system. Such being the case, the hazardous condition cannot be eliminated. Therefore, control measures must be incorporated which reduce the risk of potential accident occurrence.

From a cursory look at this inductive analysis, five initial hardware safety requirements could be established, as follows:

1) no single or common failure mode shall both arm and ignite ordnance
2) use 1 amp - 1 watt no fire EED's
3) use shielded wires
4) design electrical connectors to preclude misconnection
5) develop ordnance warning devices to indicate ordnance areas and to indicate "armed" and/or "safed" ordnance.

In the area of procedures, the need for special handling procedures and special bonding and grounding procedures would now have been established. The requirement for certified ordnance personnel would be identified as a personnel requirement. Applicable documents containing standards and requirements should be identified at this point.

It must be noted that this example is only for the purpose of familiarization and instruction and is, therefore, not entirely complete.

Figure 4-2 is an example of a PHA performed on a propulsion subsystem, where hydrazine is used as a fuel. Hydrazine, the hazardous element in this case, is both an energy source and a toxicant. The completed form is self-explanatory and is performed similarly to the first example. Figure 4-3 is a further brief example.

USE FOR TYPEWRITTEN MATERIAL ONLY

U3 4802 1434 REV. 8-65

1 SUBSYSTEM OR FUNCTION	2 MODE	3 HAZARDOUS ELEMENT	4 EVENT CAUSING HAZARDOUS CONDITION	5 HAZARDOUS CONDITION	6 EVENT CAUSING POTENTIAL ACCIDENT	7 POTENTIAL ACCIDENT	8 EFFECT	9 HAZ. CLASS	10 ACCIDENT PREVENTION MEASURES			11 VALI - DATION
									10A1 HARDWARE	10A2 PROCEDURES	10A3 PERSONNEL	
missile ordnance	transp. han-dling storage install. test flight	ordnance explosive	inclusion of the explosive into the system	explosive sub-jected to an ignition environ-ment	premature ignition signal erroneous ignition com-mand signal RFI EMP EMI excessive temperature shock electrical mis-connection	inadvertent ignition of explosive	injury to personnel damage to missile mission failure	III or IV III or IV III or IV	no single or common failure mode shall both arm and ignite ordnance use 1 amp - 1 watt no fire EED's use shielded wires design electrical con-nectors to preclude possibility of miscon-nection develop warning devices to indicate ordnance areas and to indicate armed and/or safed ordnance	establish ord-nance handling procedures, including emer-gency proce-dures establish ade-quate bonding and grounding methods	certified ordnance personnel	

Figure 4-1

1 SUBSYSTEM OR FUNCTION	2 MODE	3 HAZARDOUS ELEMENT	4 EVENT CAUSING HAZARDOUS CONDITION	5 HAZARDOUS CONDITION	6 EVENT CAUSING POTENTIAL ACCIDENT	7 POTENTIAL ACCIDENT	8 EFFECT	9 HAZ. CLASS	10 ACCIDENT PREVENTION MEASURES			11 VALI-DATION
									10A1 HARDWARE	10A2 PROCEDURES	10A3 PERSONNEL	
propulsion system	handling storage loading	hydrazine	leakage spill rupture	hydrazine is exposed to oxidizer environment	spark or flame spontaneous combustion hypergolic reaction with acids and oxidizers auto-ignition above 518°F vapor ignition above 320°F	fire or explosion	injury to personnel damage to hardware/equipment	III or IV III or IV	use materials compatible with hydrazine use non-static producing materials label and identify fuel lines use vapor detector in operations develop warning devices to indicate hydrazine areas safety showers in area breathing apparatus in area	establish handling, storage and loading procedures develop emergency procedures, including egress routes develop vapor detection procedures	protective clothing hydrazine handling training medical certification program	
			leakage spill rupture	unconfined hydrazine vapor	personnel in vicinity of unconfined hydrazine	exposure of personnel to toxic vapor	injury to personnel	III or IV	same as above	same as above	same as above	

Figure 4-2

1 SUBSYSTEM OR FUNCTION	2 MODE	3 HAZARDOUS ELEMENT	4 EVENT CAUSING HAZARDOUS CONDITION	5 HAZARDOUS CONDITION	6 EVENT CAUSING POTENTIAL ACCIDENT	7 POTENTIAL ACCIDENT	8 EFFECT	9 HAZ. CLASS	10 ACCIDENT PREVENTION MEASURES			11 VALI-DATION
									10A1 HARDWARE	10A2 PROCEDURES	10A3 PERSONNEL	
pressure tank	normal operation	compressed gas	over pressure of tank from thermal expansion or hardware fault	uncontrolled pressure relief	personnel in vicinity of uncontrolled pressure relief	contact of personnel with gas, pressure and debris	injury to personnel	III or IV	design system such that personnel and critical equipment are isolated from pressure tank incorporate pressure relief device into design	establish emergency procedures		
			manufacturing deficiency structural damage of tank		critical equipment in vicinity of uncontrolled pressure relief	contact of critical equipment with gas, pressure and debris	damage to critical equipment	III or IV	pressure indicators should be utilized tank must be proof tested before use			
					no replacement or repair, due to insufficient time or non-maintainable	loss of tank pressure	failure of systems depending upon tank pressure	II or III				

Figure 4-3

5.0 REFERENCES

A. Stack, Phillip J. (Captain, USAF), System Safety Engineering Hazard Analysis Requirements, Safety Office (SMW), SAMSO, AFSC, July 1968.

B. Harris, Roy (TRW Systems Group), Preliminary Hazard Analysis, presented at the USAF-Industry System Safety Conference, Las Vegas, Nevada, February 1969.

C. System Safety Hazard Analysis (Draft), Directorate of Aerospace Safety, Deputy Inspector General for Inspection and Safety, USAF, Norton AFB.

D. SAMSOM 127-1, Safety-Plans, Programs and Procedures, Vol. IV, System Safety Engineering, SAMSO, AFSC, March 1968.

E. MIL-STD-882, Requirements for System Safety Program for Systems and Associated Subsystems and Equipment, 15 July 1969 (Supersedes MIL-S-38130A).

USE FOR TYPEWRITTEN MATERIAL ONLY

U S 4802 1434 REV. 8-65

Unclassified

Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) The Boeing Company - Aerospace Group Aerospace Systems Division - Kent Facility P. O. Box 3999, Seattle, Washington 98124	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

System Safety Analytical Technology - Preliminary Hazard Analysis.

4. DESCRIPTIVE NOTES (Types of report and inclusive dates)

Final Report.

5. AUTHOR(S) (Last name, middle initial, last name)

C. A. Ericson

6. REPORT DATE November 28, 1962 (11) 1 Dec 62	7a. TOTAL NO. OF PAGES ~~26~~ (12) 26p.	7b. NO. OF REFS 5

8a. CONTRACT OR GRANT NO. b. nil c. nil d. nil	9a. ORIGINATOR'S REPORT NUMBERS D2-113072-1 (14) 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEMENT [redacted] U. S. Government agencies may obtain copies directly from DDC. The DDC is requested to route all other requests to Boeing for approval.

[redacted]

11. SUPPLEMENTARY NOTES Preliminary Hazard Analysis also commonly referred to as a Gross Hazard Analysis	12. SPONSORING MILITARY ACTIVITY nil

13. ABSTRACT

This document describes the method for performing a Preliminary Hazard Analysis (also known as a Gross Hazard Analysis) and using the derived results. This analysis is a method for identifying hazardous elements, hazardous conditions, and potential accidents; determining the significance of their potential effect; and establishing initial design and procedural safety requirements to eliminate or control these identified hazardous conditions and potential accidents. The data and information thereby derived can be used to serve other initial system safety needs, such as prediction, planning, and priority allocation.

DD FORM 1 NOV 65 1473
GPO 4802 1030 REV 7/66
PART 1 OF 3

Unclassified

Security Classification

357 610

14. KEY WORDS	LINK A ROLE	LINK A WT	LINK B ROLE	LINK B WT	LINK C ROLE	LINK C WT
System safety						
Hazardous element						
Hazardous condition						
Accident - potential						
Accident prevention measures						
Safety analysis						

SUPPLEMENTARY

INFORMATION

Copyright 1969 to The Boeing Company

File copy AD862338L

REV LTR A

THE BOEING COMPANY

CODE IDENT. NO. 81205

NUMBER D2-113072-1

TITLE: System Safety Analytical Technology - Preliminary Hazard Analysis

ORIGINAL RELEASE DATE _____. FOR THE RELEASE DATE OF SUBSEQUENT REVISIONS, SEE THE REVISIONS SHEET. FOR LIMITATIONS IMPOSED ON THE DISTRIBUTION AND USE OF INFORMATION CONTAINED IN THIS DOCUMENT, SEE THE LIMITATIONS SHEET.

MODEL All ASG

ISSUE NO. _____

ISSUE TO _____

PREPARED UNDER:

☐ CONTRACT NO.

☒ IR&D

☐ OTHER

PREPARED BY C. A. Ericson 12-1-69
C. A. Ericson

SUPERVISED BY H. D. Trettin 12-1-69
H. D. Trettin

APPROVED BY H. F. Eppenstein 12-1-69
H. F. Eppenstein

APPROVED BY H. D. Trettin 12-1-69
H. D. Trettin

Edited by C. R. James 11/24/69
C. R. James

U3 4802 1413 REV. 9 68

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS				SHEET NUMBER	REV LTR	ADDED SHEETS			
		SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR			SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
1	A										
2	A										
3	A										
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											

REVISIONS

LTR	DESCRIPTION	DATE	APPROVAL
A	Revised page 1 to show copyright notice. Revised pages 2 and 3 to comply.	1-22-70	[illegible]

1/28/70

U3 4802 1432 ORIG. 4/65

Unclassified

Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified).

1. ORIGINATING ACTIVITY (Corporate author) The Boeing Company - Aerospace Group Aerospace Systems Division - Kent Facility P. O. Box 3999, Seattle, Washington 98124	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

System Safety Analytical Technology - Preliminary Hazard Analysis

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Final Report; Revision A released to include copyright notice.

5. AUTHOR(S) (First name, middle initial, last name)

C. A. Ericson

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
November 28, 1969	26	5

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
b. nil	D2-113072-1
c. nil	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d. nil	

10. DISTRIBUTION STATEMENT All U. S. Government agencies may obtain copies directly from DDC. The DDC is requested to route all other requests to Boeing for approval. Ref. H. F. Eppenstein or J. W. Griswold

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
Preliminary Hazard Analysis also commonly referred to as a Gross Hazard Analysis	nil

13. ABSTRACT

This document describes the method for performing a Preliminary Hazard Analysis (also known as a Gross Hazard Analysis) and using the derived results. This analysis is a method for identifying hazardous elements, hazardous conditions, and potential accidents; determining the significance of their potential effect; and establishing initial design and procedural safety requirements to eliminate or control these identified hazardous conditions and potential accidents. The data and information thereby derived can be used to serve other initial system safety needs, such as prediction, planning, and priority allocation.

FORM DD 1 NOV 65 1473

U3 4802 1230 REV 7/66

PART 1 OF 3

Unclassified

Security Classification