Civilian Radioactive Waste
Management System

Management & Operating
Contractor

TRW Environmental Safety
Systems Inc.

YMP Site Characterization

System Safety and Human Factors

Presentation to the Nuclear Waste Technical Review Board
Arlington, VA

Lewie E. Booth
Leslie R. Eisler
June 14, 1995

Agenda

- System Safety definitions
- Extent of System Safety Analysis
- Background
- YMP System Safety Analysis (SSA) Plan
- YMP System Safety Analysis Procedure

Agenda

- Hazard tracking and risk resolution database
- Failure reporting analysis and corrective action system
- System Safety Analysis examples
- YMP Human Factors Engineering Plan
- Other activities

System Safety Definitions

- **System Safety—An engineering discipline directly related to and an integral part of design**

- **System Safety Analysis—A systematic process that identifies design-related hazards that can lead to accidents and cites specific mitigation features that are intended to eliminate or mitigate the consequences of the hazards**

- **Analysis Scope—The scope is limited to accident hazards resulting from equipment failure, design layout, or design-caused human error**

Extent of System Safety Analysis

- Construction-related work activities are excluded per DOE Order 5481.1B—Safety Analysis and Review Systems (construction organization safety)
- Designs not under M&O control such as "off-the-shelf" maintenance tools or construction equipment (construction organization safety)
- Hazards resulting from operational and maintenance procedures (these hazards are the responsibility of the M&O and are handled by way of Job Safety Analyses [JSAs])
- Non-accident related hazards such as effluent releases from normal operations and/or out-of-tolerance conditions (construction organization safety)

YMP System Safety Analysis Plan and Procedure

Background:

- 1992 Preliminary Safety Analysis Report format (non-radiological)
- 1993 Design package basis
- 1994 DOE request for System Safety Analysis Plan and Procedure

YMP System Safety Analysis Plan

Purpose:

- **Address system safety issues mandated by**
  - **DOE Order 6430.1A—General Design Criteria**
  - **DOE Order 5481.1B—Safety Analysis and Review Systems**
  - **OCRWM/YMP SEMP**
- **Describe how to accomplish objectives**

YMP System Safety Analysis Plan

General Approach:

- Based on proven analytical approaches
  - MIL-STD-882
  - SSS Handbook
- Fully developed documentation procedure and analytical process

System Safety Analysis Procedure

Describes the Following Requirements Needed to Complete a System Safety Analysis:

- **Purpose, applicability, and responsibilities**
- **Documentation procedure**
- **Analytical process**

YMP System Safety Analysis Procedure

- **Purpose**
  - **Provide methods to identify, analyze, mitigate, and monitor hazards**
- **Applicability**
  - **YMSCO and YMP teammates who accomplish or review SSAs**
- **Responsibilities**
  - **DOE, initiating organizations, M&O SS, CMO, and design**

YMP System Safety Analysis Procedure

Documentation Procedures:

- **Documentation steps**
- **Accident Analysis Summary Sheet (the key documentation being processed)**

YMP System Safety Analysis Procedure

Documentation Steps:

- **Preparing an SSA**
  - **Cover and sign-off sheets**
  - **SSWG formation**
- **Performing an SSA**
  - **Follows SSA process**
  - **Results in completed Accident Analysis Summary Sheets (scenario worksheets)**

YMP System Safety Analysis Procedure

Documentation Steps:

- **Revising an SSA**
  - **Only changed pages are issued**
  - **New Accident Analysis Summary Sheets generated where needed**

YMP System Safety Analysis Procedure

ACCIDENT ANALYSIS SUMMARY WORKSHEET (Scenario Worksheet)

SCENARIO NUMBER: SI0079 REVISION: REVISION DATE:

LOCATION:

SCENARIO:

SYSTEM/COMPONENT FAILURE:

ACCIDENT CLASSIFICATION:

Frequency Rating:

Consequence Rating:

Risk Designation:

MITIGATION/CONTROL FEATURES:

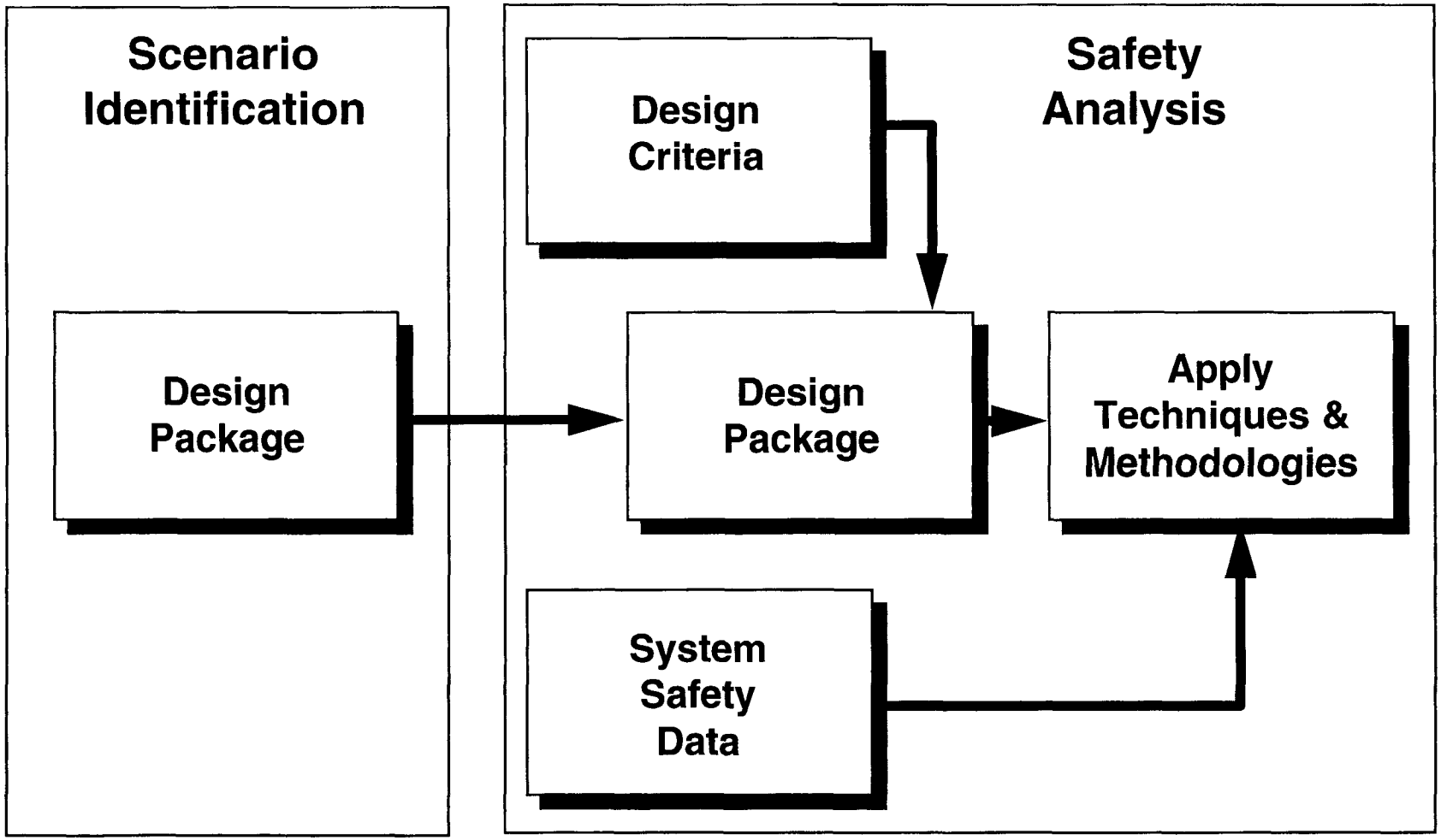
MITIGATION DOCUMENTATION:

YMP System Safety Analysis Procedure

Safety System Analysis Process:

- **Safety assessment**
- **Mitigation of hazards**
- **SSWG interfaces**

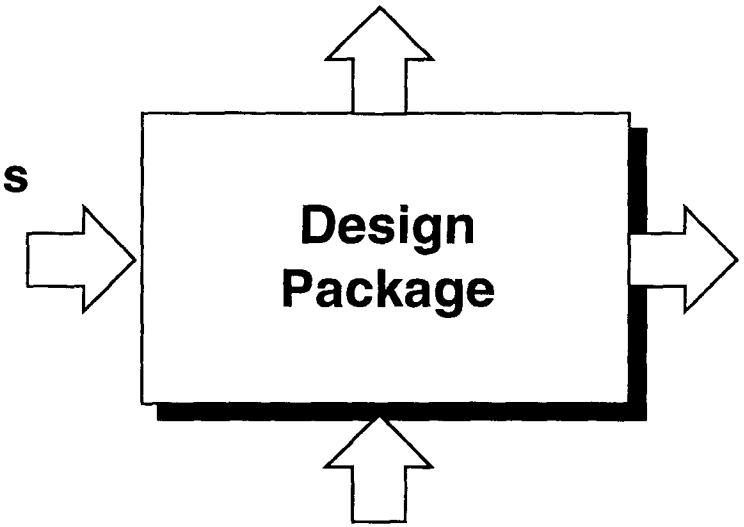
YMP System Safety Analysis Procedure
System Safety Assessment



YMP System Safety Analysis Procedure
System Safety Assessment

Scenario Identification

Type I: Accident Scenarios
Potential accidents resulting from equipment failure, design layout, or design-caused human error

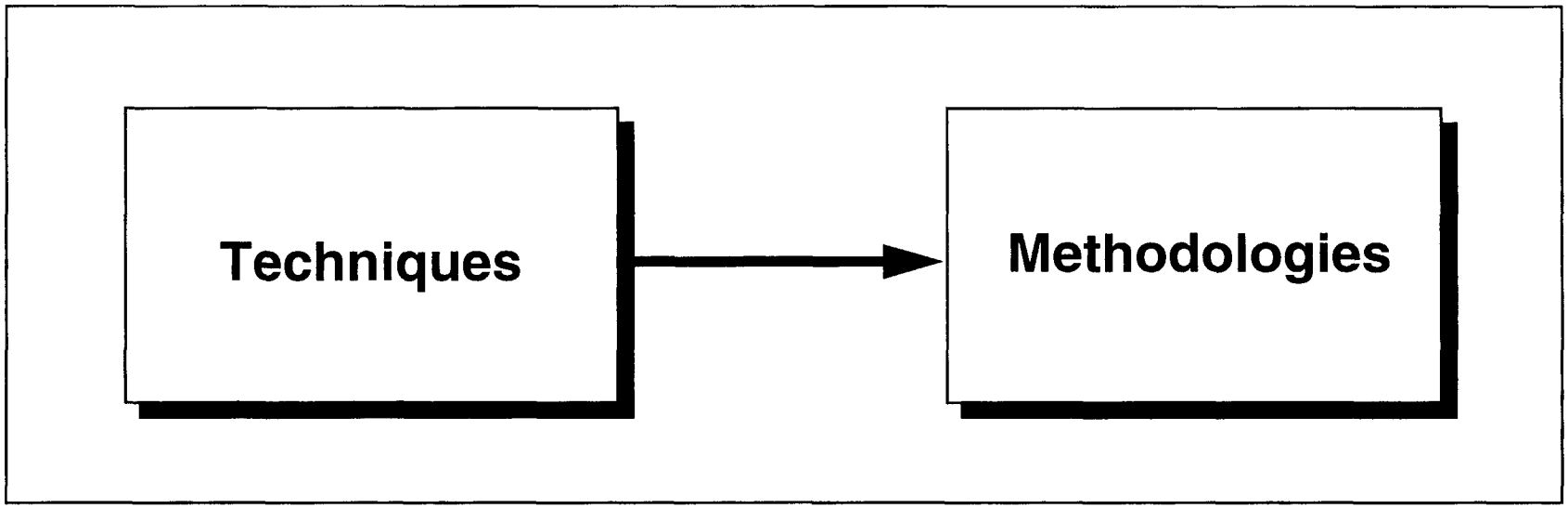


Energy and materials *unintentionally* introduced into the system

Type II: Health Scenarios
Health hazards due to normal operation or operation in out-of-tolerance conditions

Energy and materials *intentionally* introduced into the system

YMP System Safety Analysis Procedure System Safety Assessment



- Scenario analysis
- Hazards analysis
- Human factors analysis
- Failure modes effects and criticality analysis

- Comparative analysis
- Absolute analysis
- Subjective analysis

YMP System Safety Analysis Procedure
System Safety Analysis Process

System Safety Mitigation:

- Review and agreement on mitigation followed by sign-off
- Hazard control, mitigation implementation, and tracking

Hazard Tracking and Risk Resolution Database

- "Ingres" database
- Scenario worksheets
- Data entry
- Follow-up

Failure Reporting Analysis and Corrective Action Database (FRACAS)

- Maintenance centered database
- Specialized reports
- Corrective actions
- Integrated Logistics Support

System Safety Analysis Examples

TBM System Safety Analysis:

- Type of analyses
- Risk methodology
- SSWG

System Safety Analysis Examples

- System Safety Society Manual
- Type of analyses used
  - Scenario Analysis
  - Hazards Analysis
  - Human Factors Analysis
  - Failure Mode Effects and Criticality Analysis
  - Job Safety Analysis

System Safety Analysis Examples—TBM SSA

Risk Methodology:

- Fourteen steps
- Threats checklist
- Hazard frequency
- Hazard consequence
- Risk matrix

System Safety Analysis Examples—TBM SSA

System Safety Working Group:

- Establish for each System Safety Analysis
- Cross section representation
- System Safety Analysis review
- Final sign-off for technical content

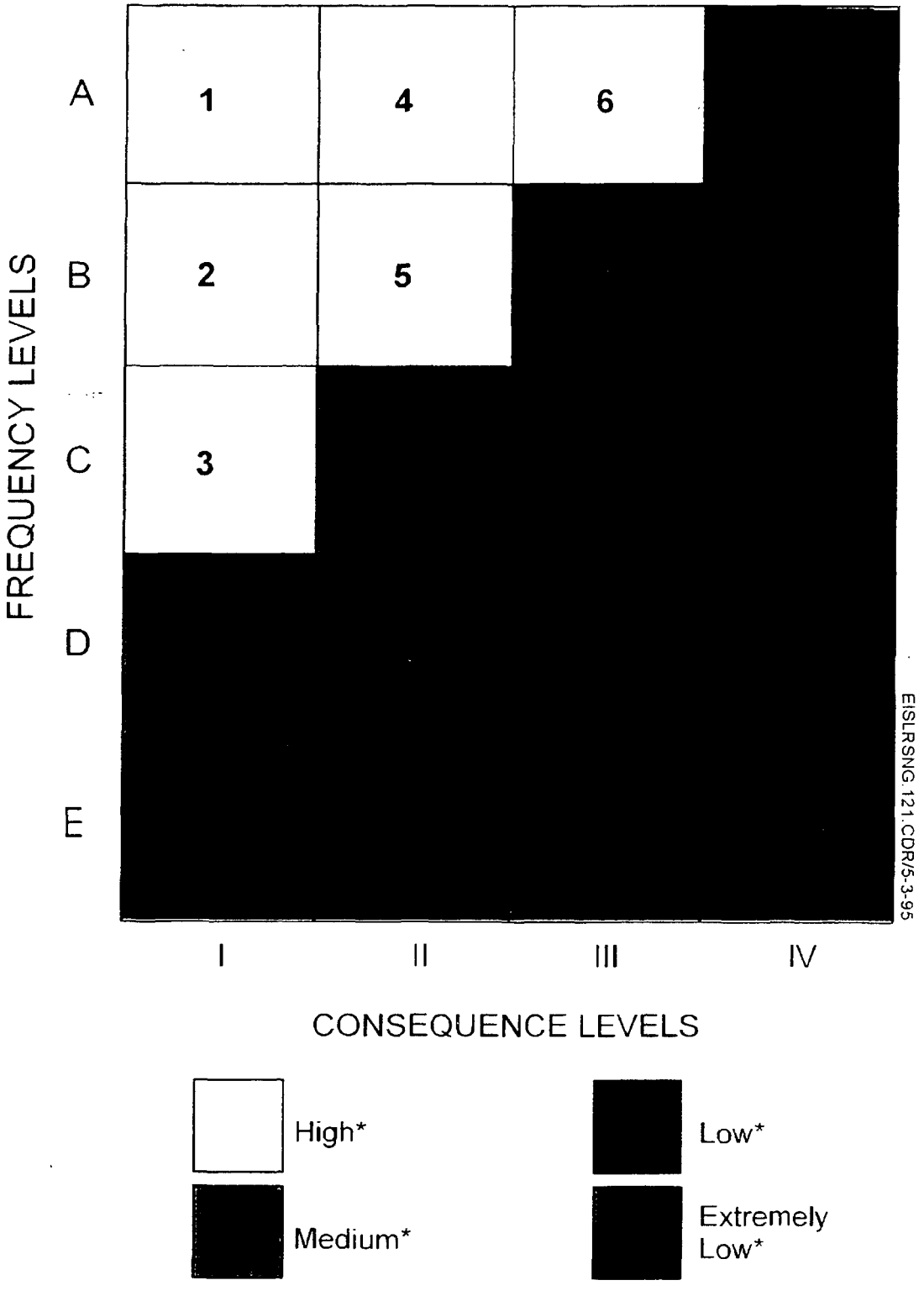
Frequency Rating Scale

Frequency	Description
A Frequent	Likely to occur frequently in the life of an SSC*
B Probable	Likely to occur several times in the life of an SSC*
C Occasional	Likely to occur some time in the life of an SSC*
D Remote	Unlikely but possible to occur in the life of an SSC*
E Improbable	So unlikely, it can be assumed occurrence may not be experienced in the life of an SSC*
	*System/structure/component
Frequent	> 4.5 occurrences or more than one occurrence per year
Probable	> 2.25 but not more than 4.5 occurrences or one or fewer occurrences per year during TBM lifetime
Occasional	> 1.0 but not more than 2.25 occurrences during TBM lifetime
Remote	> .25 but not more than 1.0 occurrence during TBM lifetime

Consequence Rating and Definition

Consequence Level		Maximum Consequence
I	Catastrophic	Death, system/equipment loss, or several environmental impact
II	Critical	Severe injury or illness, major system/ equipment or environmental damage
III	Marginal	Minor injury or illness, minor system/ equipment damage, minor delay of data collection or loss of data
IV	Negligible	Less than minor injury, occupational illness, or system damage

Risk Rating Matrix

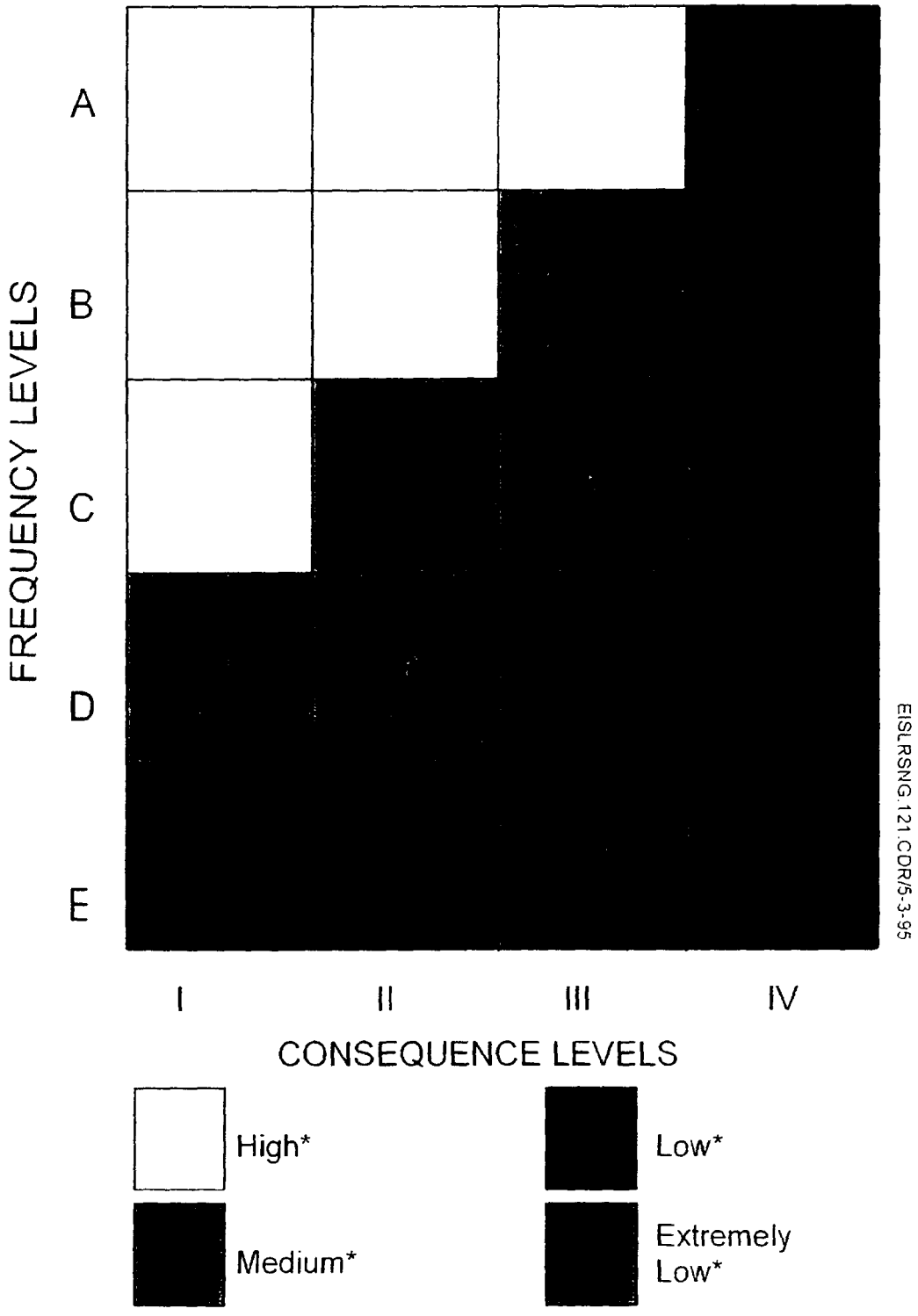


Civilian Radioactive Waste Management & Operating System

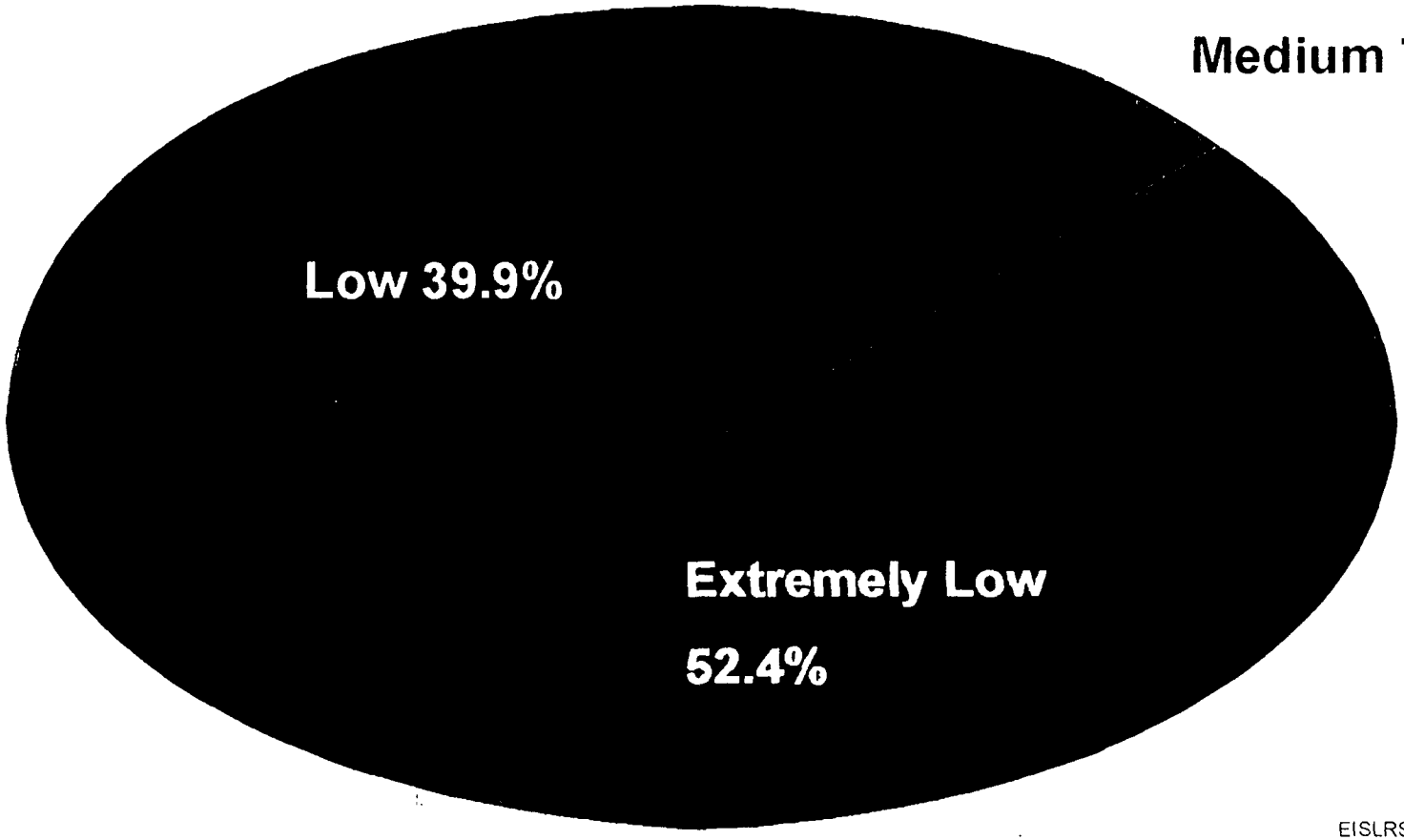
Management & Operating Contractor

6-14-95

Scenarios Distributed Over Risk



Percentage of TBM Scenarios by Level of Risk



EISLRSNG.121.CDR/5-3-95

System Safety Analysis Examples

Control Precedence:

- Eliminate hazards by design
- Addition of safety features and devices
- Use warning and alerting devices
- Establish procedures/train personnel

System Safety Analysis Examples

- TBM
- Conveyor
  - Surface
  - Subsurface

System Safety Analysis Examples

Design Package 1C:

- Surface compressed air
- Standby generators

System Safety Analysis Examples

Design Package 1D:

- Muck storage area
- Conveyor access road
- Compressed air
- Lighting, fencing, and piping
- Pads and foundations

System Safety Analysis Examples

Design Package 2B:

- Subsurface ventilation
- Subsurface trolley

System Safety Analysis Examples

Design Package 2C:

- North ramp excavation
- Support areas
- Subsurface water
- Subsurface compressed air
- Ground support
- Subsurface lighting
- Ventilation
- Subsurface rail
- Fire detection and protection
- North ramp walkway*

* Separate trade-off study

System Safety Analysis Examples

TBM:

- Additional conveyor emergency stop cord
- Relocation of segment hoist controls
- Addition of safety gates
- Labeling controls (permanent, function, settings/values)
- Definition of "master-slave" control relationship

System Safety Analysis Examples

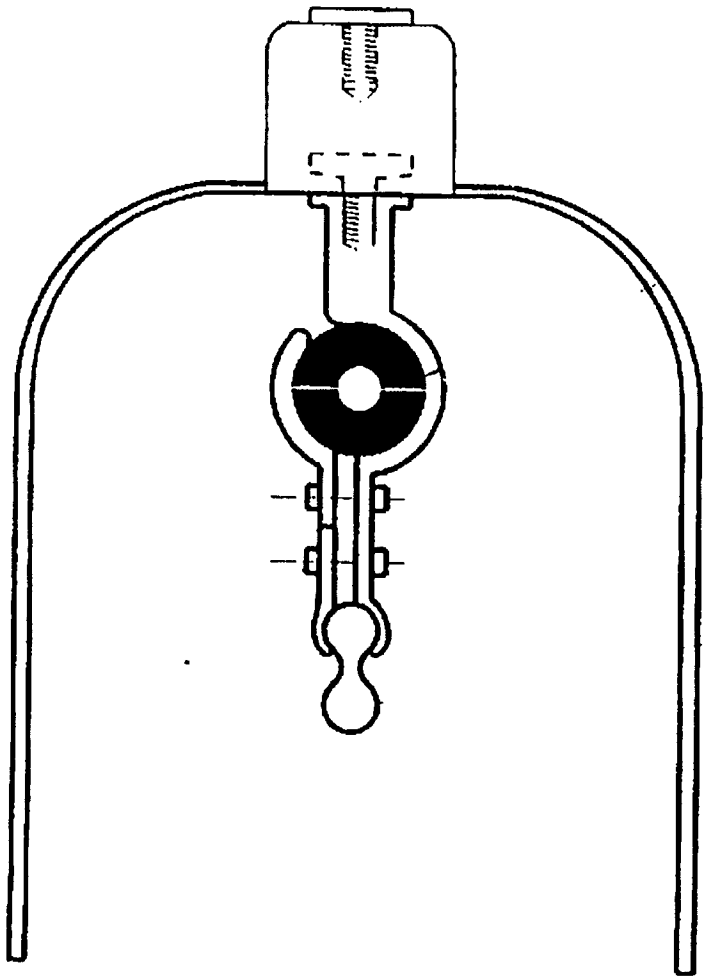
Work Platforms:

- Guardrails and handrails
- Toe kicks
- Adequate lighting
- Non-skid surfaces
- Access ladders per OSHA/MSHA

System Safety Analysis Examples

- **Ventilation system**
  - **Performance monitoring (e.g., temperature, vibration)**
  - **Fan access port to remove debris**
- **Trolley or train**
  - **Personnel and equipment restraints**
  - **"Deadman" controls**
  - **Redundant brakes**

Trolley Pentograph



Trolley Guard Insulated Fire-Retardant Material

System Safety Analysis Examples

Tunnel:

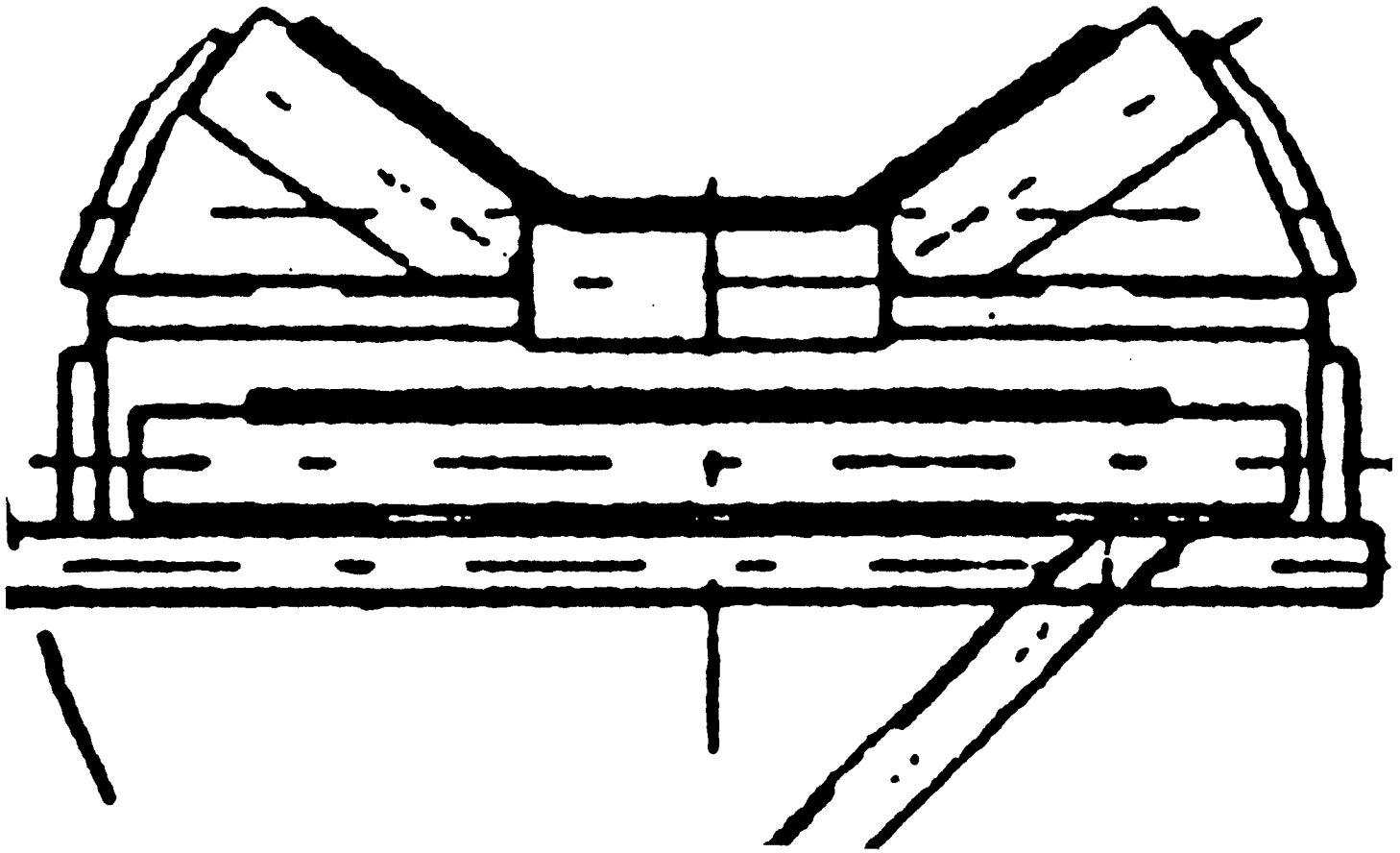
- Location of utilities and protective barriers
- Adequate lighting
- Warning signs and signals (e.g., train travel lights)
- Training and procedures
  - Personnel exclusion zones
  - Personnel access (e.g., walkways)
  - Personnel Protective Equipment
  - Vehicle travel speeds (e.g., trolley)

System Safety Analysis Examples

Conveyor:

- Emergency shut down controls
- Lockouts and tagouts
- Covers, belt angle, flashing, and load limits to prevent muck from being ejected
- Start-up signal
- Operator training

SUBSURFACE CONVEYOR



YMP Human Factors Engineering Plan

Maximize Human Performance:

- Reduce errors
- Increase productivity
- Decrease damage
- Improve safe operation and maintenance

YMP Human Factors Engineering Plan

- Address HFE issues mandated by
  - DOE Order 6430.1A—General Design Criteria
  - UCRL-AR-108791—Human Factors Engineering Standards for Use in Design, Modification, and Evaluation of DOE Nuclear Facilities: Vol. 1
- Basis
  - MIL-H-46855
  - MIL-STD-1472
  - ANSI/HFS-100/1988
  - Americans with Disabilities Act Guidelines
  - DOE-STD-1062-94 (draft)

Plans/Status

YMP Human Factors Engineering Plan:

- Being developed
- Draft completion date July 1995

Human Factors Engineering Activities

- Requirements definition and analysis
- Special and trade studies
- Design inputs
- System Safety support
- Task identification and procedure development

Other System Safety and Human Factors Engineering Activities

- Reviews
  - Specifications
  - Drawings
  - Analyses
- Configuration Control Board

Other System Safety and Human Factors Engineering Activities

- TBM walk down
- Special studies
  - Track switches
  - Walkways and niches
  - TBM mapping gantry follow-up
  - ACD

Other Activities

- Poster session
- Future plans
- Staffing