# Status of Systems Safety and Human Factors Planning

M. Gregory Smith
U.S. Department of Energy
Management & Operating Contractor

Presented to

Nuclear Waste Technical Review Board
March 10, 1992

# TOPICS

- ENVIRONMENTAL, HEALTH AND SAFETY PLAN
- SYSTEM SAFETY
- HUMAN FACTORS ENGINEERING

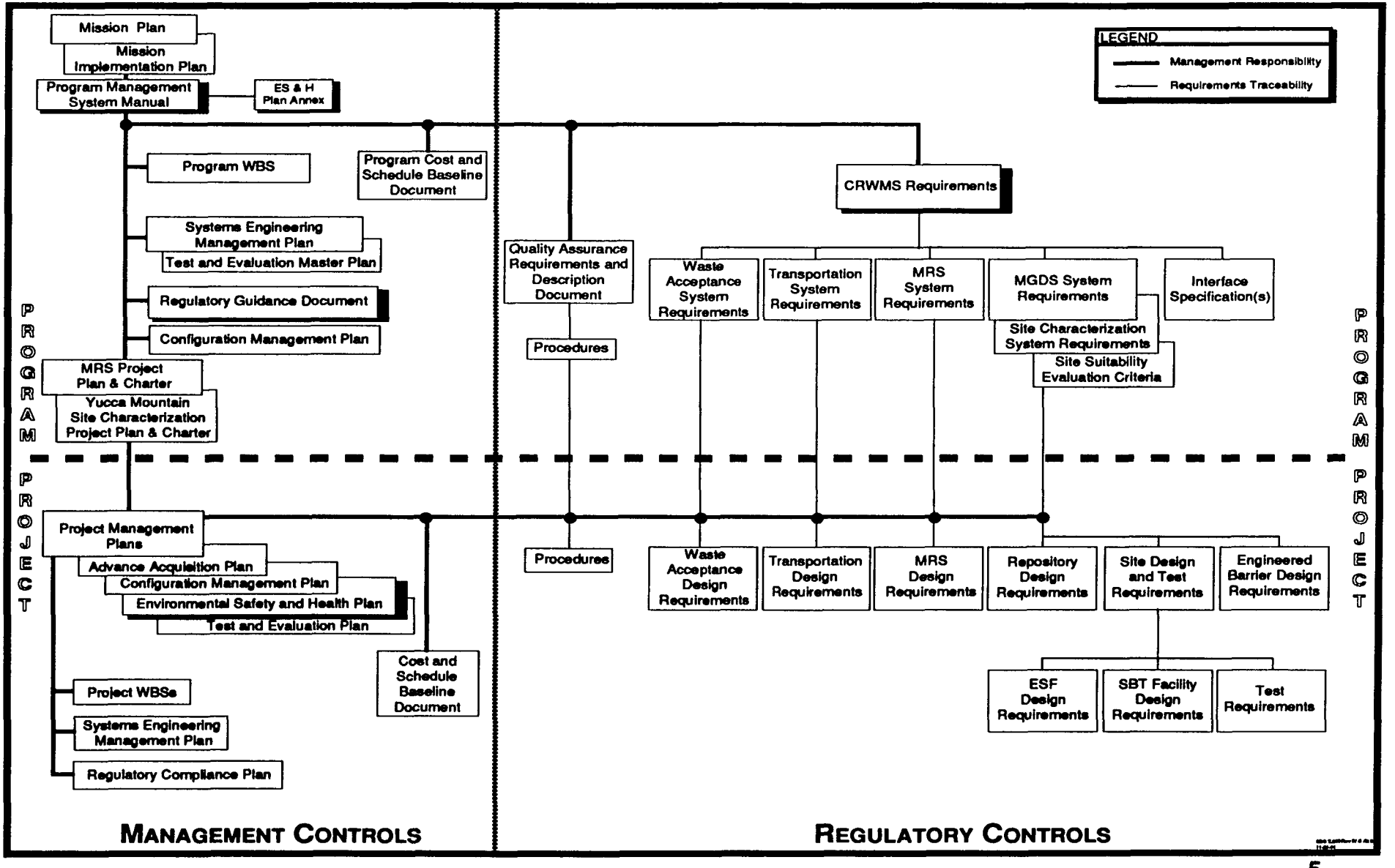
# ENVIRONMENTAL, HEALTH AND SAFETY PLAN

# ENVIRONMENTAL, HEALTH AND SAFETY PLAN

- IDENTIFIES SYSTEM SAFETY PROCESSES AND ORGANIZATIONAL RESPONSIBILITIES
- COORDINATED WITH THE M&O REQUIREMENTS AND LICENSING ORGANIZATION
- MODELED AFTER MIL-STD-882B AND COMPLIANT WITH DOE ES&H GUIDANCE*
- PROGRAM-LEVEL PLAN
- SCOPE - ALL ASPECTS OF SAFETY

*Anticipating a transition to NRC regulations in Title 10 of CFR, Chapter I

# DOCUMENT HIERARCHY



# FEDERAL REGULATORS*

**SAFETY**

| | Radiation | Chemical | Physical |
|---|---|---|---|
| **On-site Worker Safety** | NRC | DOL-OSHA<br>DOE | DOL-OSHA -MSHA<br>DOE |
| **Off-site Public Safety** | NRC<br>EPA | EPA<br>FEMA<br>DOT<br>DOE | EPA<br>FEMA<br>DOT<br>DOE |

*Major regulators shown, not exhaustive. State and local regulators not shown, site specific.

# SYSTEM SAFETY

# SAFETY DEFINITION

- FREEDOM FROM THOSE CONDITIONS THAT CAN CAUSE DEATH, INJURY, OCCUPATIONAL ILLNESS, HARM TO THE ENVIRONMENT, DAMAGE TO OR LOSS OF EQUIPMENT OR PROPERTY*

*Adapted from SYSTEM SAFETY ENGINEERING AND MANAGEMENT by Roland and Moriarty

# SYSTEM SAFETY OBJECTIVES*

- POTENTIAL HAZARDS ARE SYSTEMATICALLY IDENTIFIED
- POTENTIAL CONSEQUENCES ARE ANALYZED
- REASONABLE MEASURES TO ELIMINATE, CONTROL, OR MITIGATE THE HAZARDS HAVE BEEN TAKEN, INCLUDING WHERE APPLICABLE, COMPLIANCE WITH COMMITMENTS MADE IN ENVIRONMENTAL ASSESSMENTS AND IMPACT STATEMENTS

* DOE Order 5481.1B

# SYSTEM SAFETY APPROACH

- PERFORM AS AN INTEGRATED PART OF THE SYSTEMS ENGINEERING PROCESS
- INTEGRATION OF REQUIREMENTS FROM REGULATORY ANALYSIS
- ALLOCATION OF REQUIREMENTS TO PROJECTS
- WRITE PROJECT-LEVEL ES&H PLAN
- PERFORM HAZARD ANALYSES
- ESTABLISH SYSTEM SAFETY WORKING GROUP
- PARTICIPATE IN DESIGN ACTIVITIES
- AUDITS AND REVIEWS TO ENSURE VERIFICATION OF THE DESIGN REQUIREMENTS
- MODELED AFTER MIL-STD-882B*

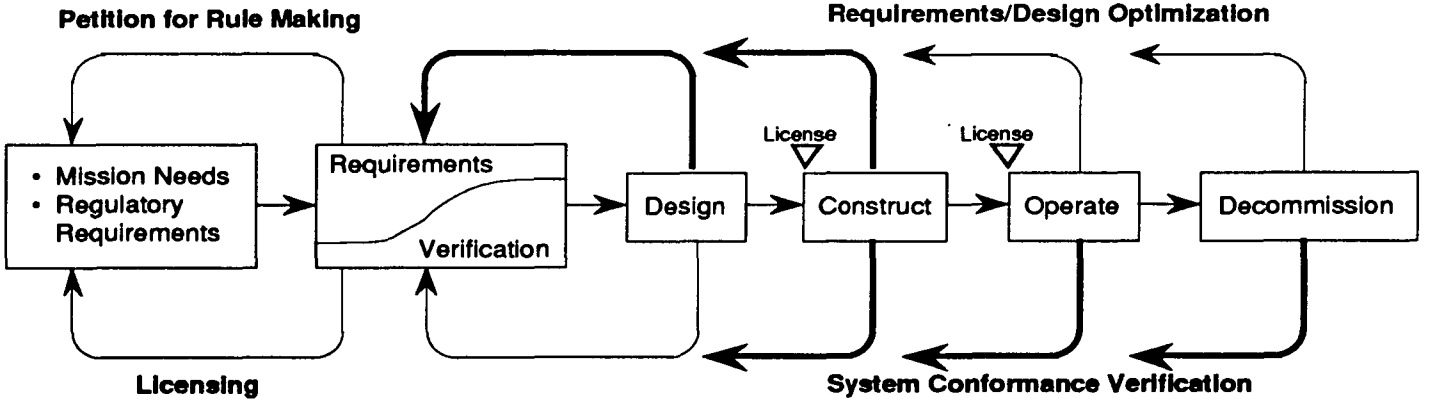
| Program | Project |
|---|---|
| ✓ | |
| ✓ | |
| ✓ | |
| | ✓ |
| | ✓ |
| ✓ | ✓ |
| | ✓ |
| ✓ | ✓ |

*Cited by DOE Order 5481.1B

# SYSTEMS ENGINEERING PROCESS

**Requirements Analysis**

- Functional Analysis and Requirements Allocation
- Design Synthesis and Integration
- Evaluation and Optimization
- System Definition




**Licensing**

- Annotated Outline
- License Application

**Verification**

- Technical Reviews
- Risk Management
- Configuration Management
- Test and Evaluation
- Software V & V
- Regulatory Compliance
- Performance Assessment

T.403

# HAZARD ANALYSIS *

**A SYSTEMATIC STUDY OF A SYSTEM OPERATION TO IDENTIFY HAZARDS AND MAKE RECOMMENDATIONS FOR THEIR ELIMINATION, CONTROL, OR MITIGATION DURING ALL LIFE-CYCLE PHASES**

*** Adapted from DOE Order 5481.1B**

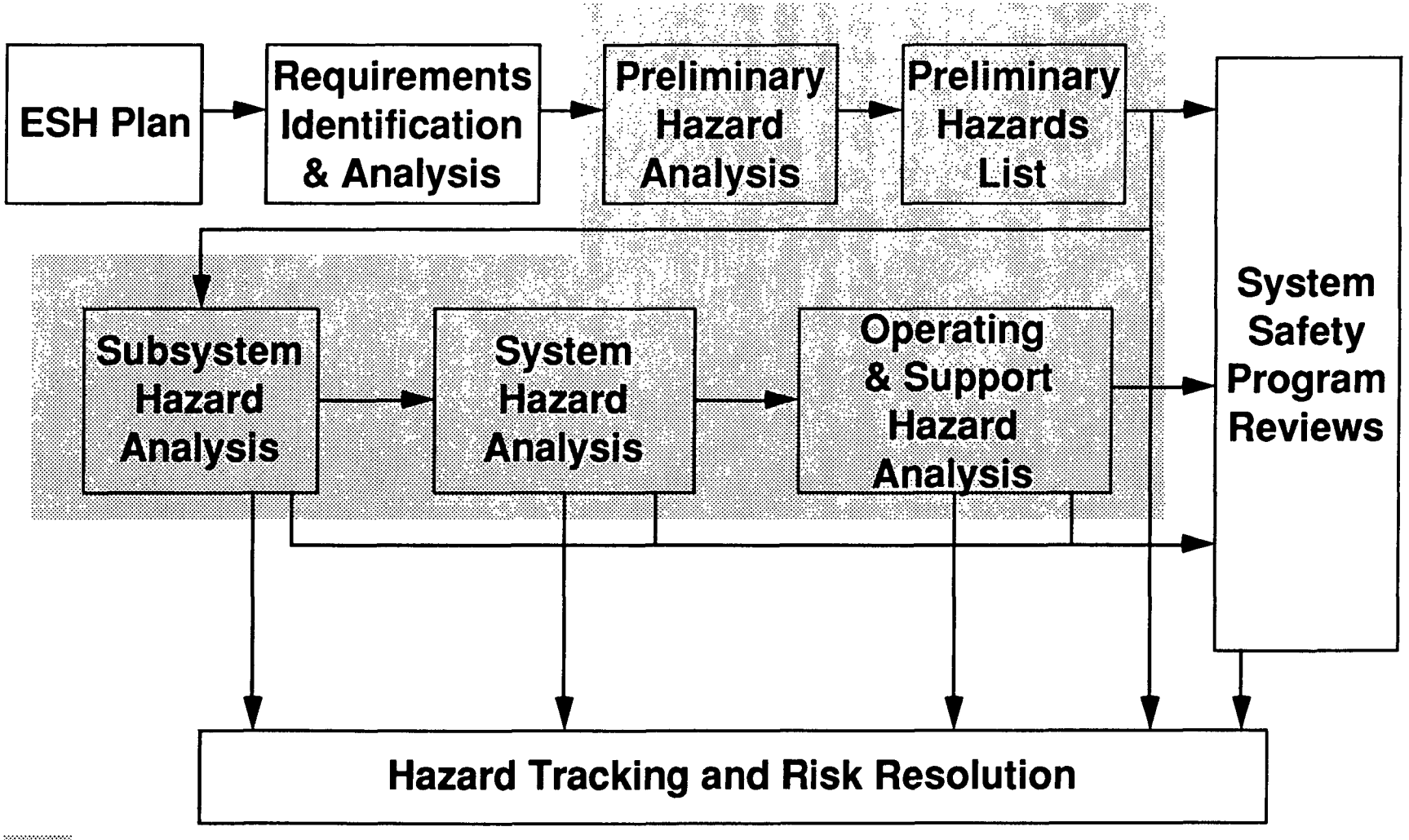
# HAZARD ANALYSIS PROCESS

- IDENTIFY HAZARDS AND THE ROOT CAUSES
- DETERMINE HAZARD PROBABILITIES /CONSEQUENCES
- RECOMMEND CORRECTIVE ACTION TO RESOLVE DESIGN PROBLEMS AND CORRECT PROCEDURES
- PROVIDE DOCUMENTED EVIDENCE OF COMPLIANCE WITH DESIGN, CODE OR SPECIFICATION REQUIREMENTS TO MANAGEMENT

# HAZARDS WILL BE QUANTIFIED

- PROBABILISTIC RISK ASSESSMENT TECHNIQUES WILL BE USED
- HUMAN ERROR, EQUIPMENT FAILURE, AND EXTERNAL EVENTS WILL BE CONSIDERED
- REQUIRES STATISTICS ON ACCIDENTS, HUMAN ERROR, NATURAL EVENTS, AND DELIBERATE EVENTS

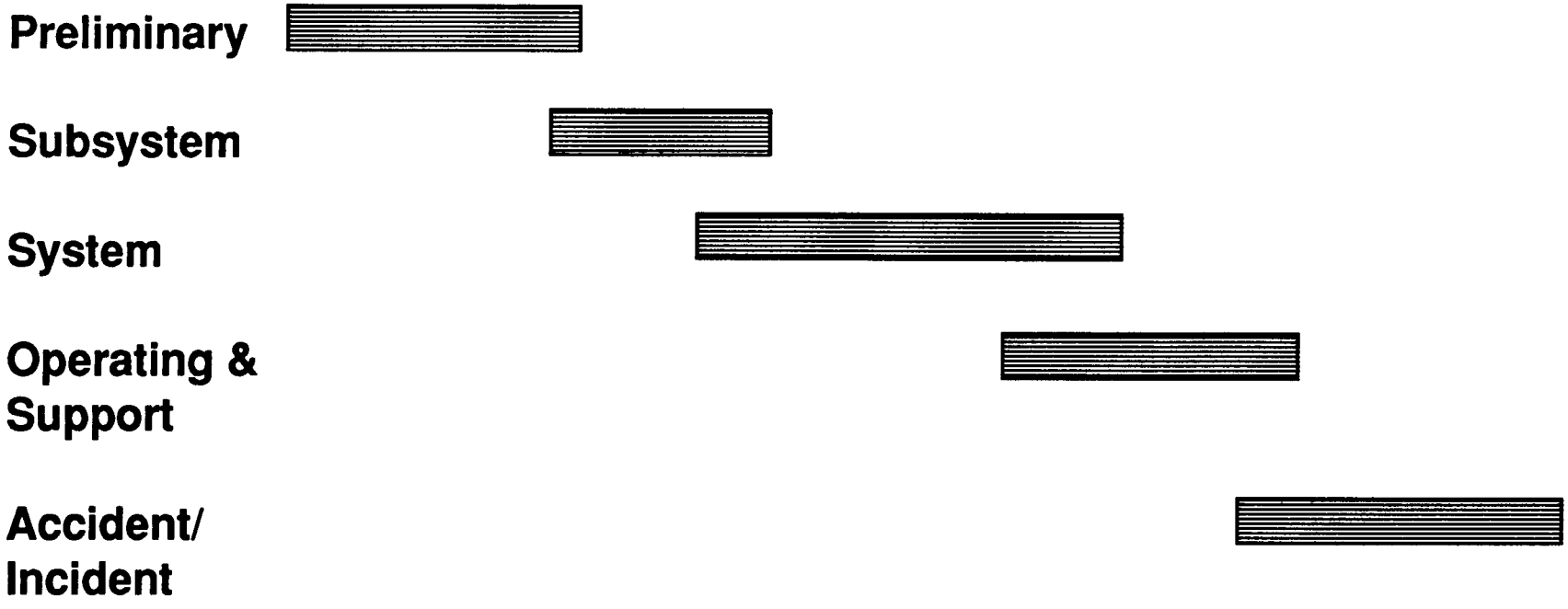
# SYSTEM SAFETY ACTIVITIES



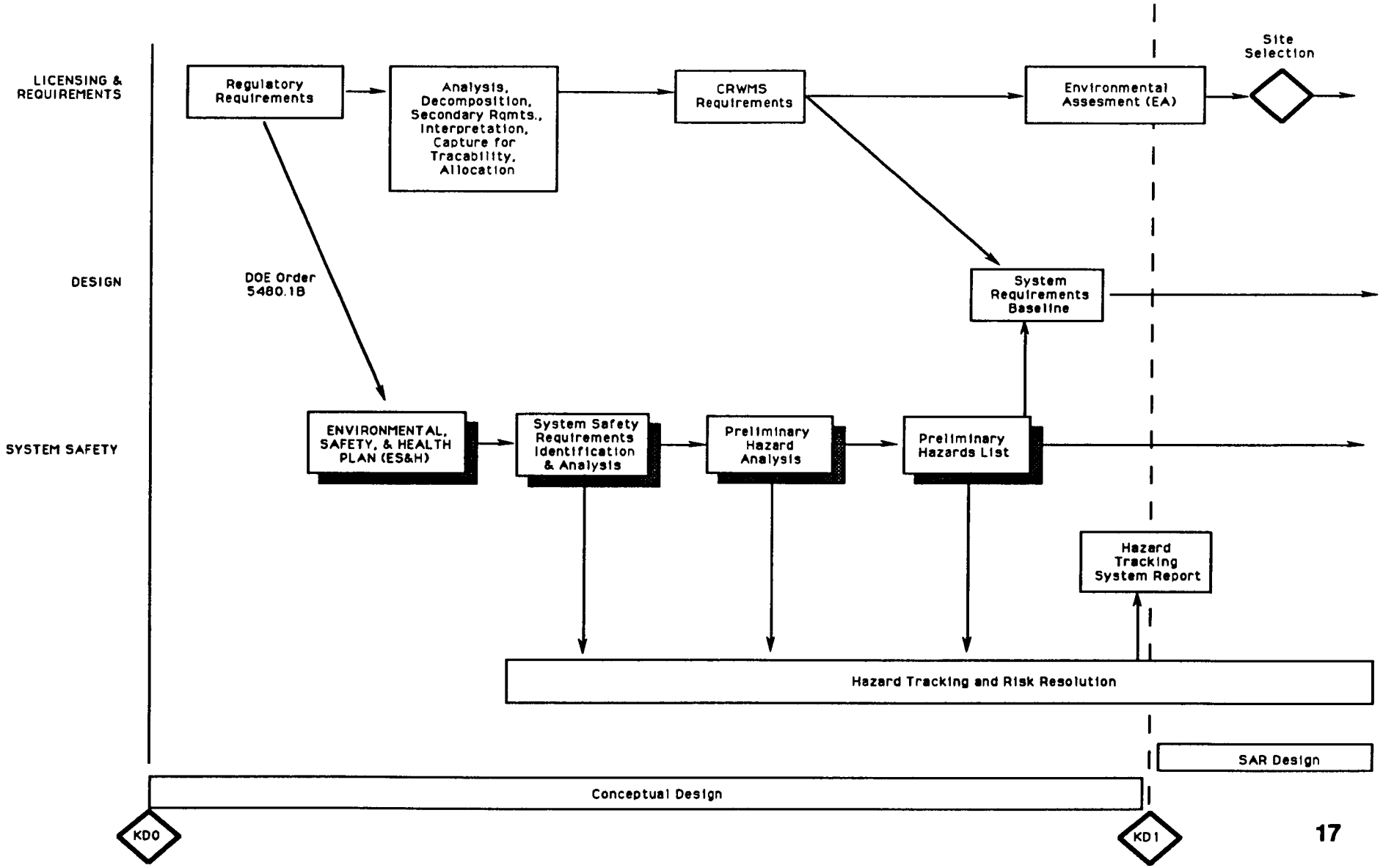

= Affects design and SAR

# HAZARD ANALYSES & PROGRAM PHASES

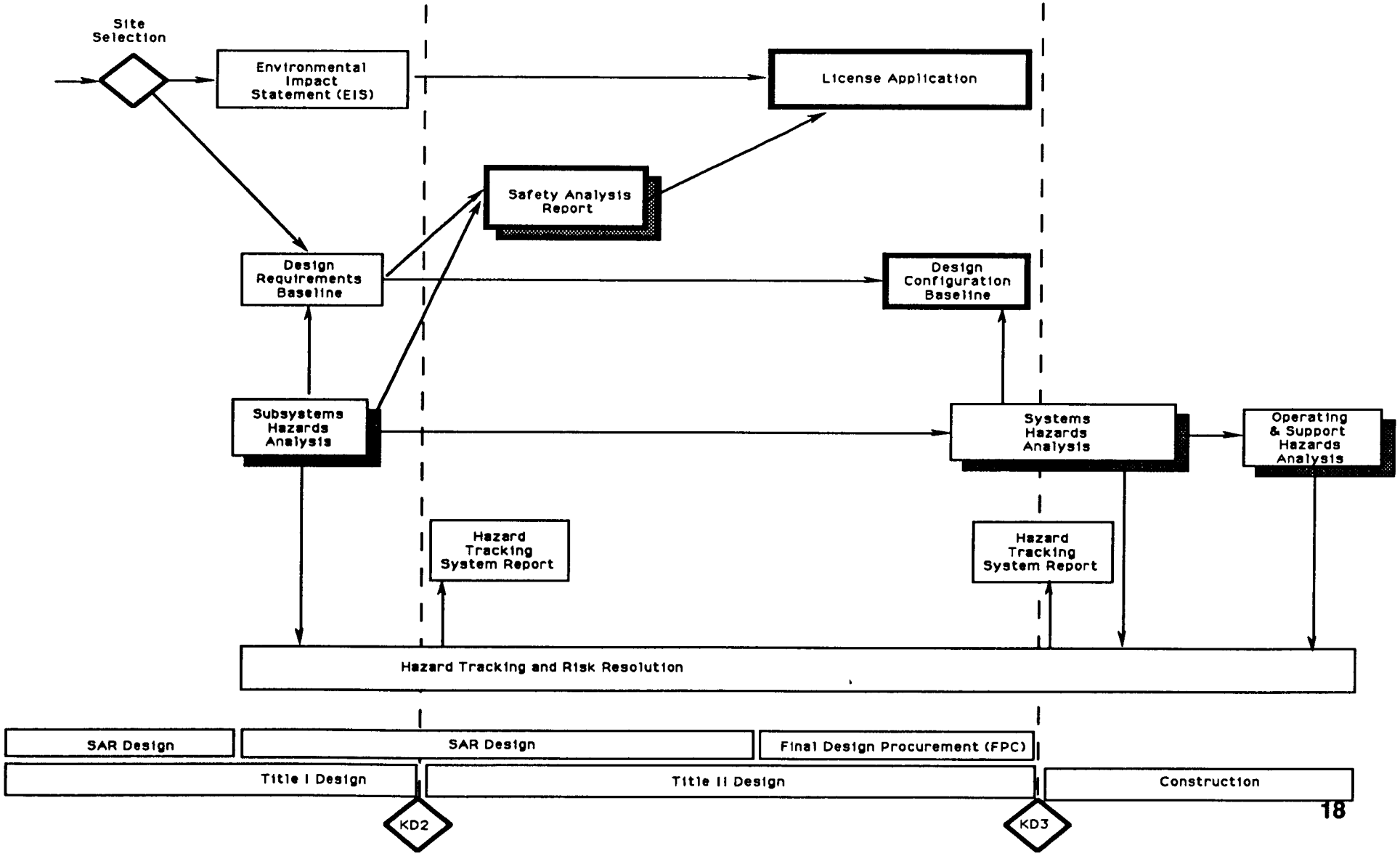
| Conceptual Design | Design | Construction | Test | Operations |
|---|---|---|---|---|



# SS AND REQ & LIC ACTIVITIES



# SS AND REQ & LIC ACTIVITIES (CON'T)



# SYSTEM SAFETY TASK DEFINITIONS

- PRELIMINARY HAZARD ANALYSIS - OVERALL ASSESSMENT OF RISK AND IDENTIFICATION OF SAFETY CRITICAL AREAS NEEDING DETAILED STUDY

- SUBSYSTEM HAZARD ANALYSIS - IDENTIFICATION OF HAZARDS ASSOCIATED WITH COMPONENT FAILURES AND FUNCTIONAL RELATIONSHIPS WITH OTHER COMPONENTS OR EQUIPMENT IN A GIVEN SYSTEM

- SYSTEM HAZARD ANALYSIS - EXAMINATION OF THE INTERFACES IDENTIFIED IN SUBSYSTEM ANALYSIS, INCLUDES SOFTWARE INTERFACES

- OPERATING AND SUPPORT HAZARD ANALYSIS - INCLUSION OF THOSE FACTORS IN THE OPERATING ENVIRONMENT WHICH CAN DEGRADE THE SYSTEM

# SYSTEM SAFETY TASK DEFINITIONS (CON'T)

- ACCIDENT-INCIDENT ANALYSIS - ANALYSES OF ACCIDENTS OR INCIDENTS TO DETERMINE THEIR CAUSE AND WHAT CHANGES TO THE DESIGN OR PROCEDURES ARE REQUIRED

- HAZARD TRACKING - LOGGING OF IDENTIFIED AND ACTUAL HAZARD. MAINTAINED THROUGH ALL LIFE-CYCLE PHASES. MAINTAINED IN A DATA BASE. DATA BASE CAN BE QUERIED FOR TRENDS.

# SYSTEM SAFETY RESULTS

- HIGH DEGREE OF PUBLIC HEALTH AND SAFETY
- HIGH DEGREE OF OCCUPATIONAL HEALTH AND SAFETY
- IMPROVED PUBLIC ACCEPTANCE TOWARD SYSTEM
- REDUCED CLAIMS AND COMPENSATION
- INCREASED AVAILABILITY

# HUMAN FACTORS ENGINEERING

# HUMAN FACTORS ENGINEERING DEFINITION

- NUREG-0700: THE SCIENCE OF OPTIMIZING THE PERFORMANCE OF HUMAN BEINGS

- EPRI NP-3659: A DISCIPLINE CONCERNED WITH THE SYSTEMATIC STUDY AND APPLICATION OF WHAT'S KNOWN ABOUT HUMAN BEHAVIOR TO SYSTEM DEVELOPMENT DECISIONS

# HFE OBJECTIVES

- DOE 6430.1A: HUMAN FACTORS ENGINEERING PRINCIPLES SHALL BE INTEGRATED INTO THE DESIGN OF SYSTEMS AND THE FACILITIES THAT HOUSE AND SUPPORT THESE SYSTEMS

---

- REDUCE PROBABILITY OF ERROR
- REDUCE RISKS TO PUBLIC AND WORKERS
- INCREASE PRODUCTIVITY
- DEVELOP DESIGN REQUIREMENTS THAT TAKE ADVANTAGE OF HUMAN CAPABILITIES AND AVOID HUMAN LIMITATIONS TO OPTIMIZE HUMAN PERFORMANCE

# HUMAN FACTORS ENGINEERING APPROACH

- INTEGRATED INTO THE SYSTEMS ENGINEERING PROCESS
- ENSURE THAT APPLICABLE REQUIREMENTS ARE PLACED INTO THE TECHNICAL BASELINE
- WORK CLOSELY WITH SYSTEM SAFETY, RAM, AND REQUIREMENTS AND LICENSING IN PERFORMING HAZARD ANALYSES
- PARTICIPATE IN DESIGN PROCESS, AUDITS AND REVIEWS

# HFE TASKS *

| | Program | Project |
|---|---|---|
| • DOCUMENT PROGRAM-LEVEL REQUIREMENTS | ✓ | |
| • ALLOCATE REQUIREMENTS TO PROJECTS | ✓ | |
| • DEVELOP DETAILED OPERATIONAL CONCEPTS | | ✓ |
| • ALLOCATE REQUIREMENTS TO MAN OR MACHINE | | ✓ |
| • PERFORM TASK, SKILLS AND ERROR ANALYSES | | ✓ |
| • PARTICIPATE IN DESIGN PROCESS | | ✓ |
| • PERFORM TEST & EVALUATIONS. AUDITS & REVIEWS | ✓ | ✓ |
| • DEVELOP PROCEDURES | | ✓ |
| • DEVELOP TRAINING MATERIALS | | ✓ |

*Examples, not exhaustive

# PROGRAM-LEVEL REQUIREMENTS

- DRAFT PROGRAM-LEVEL HFE REQUIREMENTS HAVE BEEN DOCUMENTED
- REFERENCES SIX REQUIREMENTS DOCUMENTS
- TWENTY-ONE CATEGORIES OF REQUIREMENTS

# REFERENCED REQUIREMENTS DOCUMENTS

- GUIDELINES FOR CONTROL ROOM DESIGN REVIEW, NUREG-0700
- HUMAN FACTORS DESIGN GUIDELINES FOR MAINTAINABILITY OF DEPARTMENT OF ENERGY NUCLEAR FACILITIES, UCRL-15673
- DOE GENERAL DESIGN CRITERIA, DOE Order 6430.1
- AMERICAN NATIONAL STANDARD FOR HUMAN FACTORS ENGINEERING OF VISUAL DISPLAY TERMINAL WORKSTATIONS, ANSI/HFS STANDARD No. 100-1988
- HUMAN ENGINEERING DESIGN CRITERIA FOR MILITARY SYSTEMS, EQUIPMENT AND FACILITIES, MIL-STD-1472D
- GUIDELINES FOR DESIGNING USER INTERFACE SOFTWARE. MITRE. SMITH AND MOSIER.

# HFE REQUIREMENTS CATEGORIES

- ANTHROPOMETERY
- ALARMS/WARNING SYSTEMS
- AUDIO DISPLAYS
- CONTROLS
- CONTROL-DISPLAY INTEGRATION
- ENVIRONMENTAL CONDITIONS
- EMERGENCY LIGHTING
- HAZARDS AND SAFETY
- HEAD-UP DISPLAY
- LABELS AND LOCATION AIDS
- MAINTAINABILITY

# HFE REQUIREMENTS CATEGORIES (CON'T)

- OPERATIONAL VEHICLES
- PANEL LAYOUT
- PROTECTIVE EQUIPMENT
- REMOTE HANDLING
- SMALL SYSTEMS AND EQUIPMENT/PORTABILITY
- USER-COMPUTER INTERFACE
- VISUAL DISPLAYS
- VISUAL DISPLAY TERMINAL WORKSTATION
- VOICE COMMUNICATIONS
- WORKPLACE LAYOUT

# HFE RESULTS

- DECREASED PROBABILITY OF HUMAN ERROR LEADING TO

  - DECREASED PROBABILITY OF ACCIDENT

  - INCREASED PRODUCTIVITY

  - INCREASED AVAILABILITY

  - MORE USABLE DESIGN

# SUMMARY

- ENVIRONMENTAL, SAFETY AND HEALTH PLAN IS BEING DEVELOPED
- SYSTEM SAFETY AND HUMAN FACTORS ENGINEERING ARE PART OF THE SYSTEMS ENGINEERING PROCESS
- HUMAN FACTORS ENGINEERING REQUIREMENTS ARE BEING DOCUMENTED IN THE TECHNICAL BASELINE

# REQUIREMENTS APPENDIX *

## GENERAL SAFETY OPERATIONS

- DOE 5480.1B, ENVIRONMENTAL, SAFETY AND HEALTH PROGRAM FOR DOE OPERATIONS
- DOE 5481.1B, SAFETY ANALYSIS AND REVIEW SYSTEM
- DOE 5482.1B, ENVIRONMENTAL, SAFETY AND HEALTH APPRAISAL PROGRAM
- DOE 5000.3, UNUSUAL OCCURRENCE REPORTING SYSTEM

## Radiological Safety Operations

- DOE Order 5480.5, SAFETY OF NUCLEAR FACILITIES
- DOE Order 5480.11, RADIATION PROTECTION FOR OCCUPATIONAL WORKERS
- 10 CFR Part 20, STANDARDS FOR PROTECTION AGAINST RADIATION

*Examples of orders and regulations. Not exhaustive.

# REQUIREMENTS (CON'T)

- 10 CFR Part 60, DISPOSAL OF HIGH-LEVEL RADIOACTIVE WASTES IN GEOLOGIC REPOSITORIES
- 10 CFR Part 72, LICENSING REQUIREMENTS FOR THE STORAGE OF SPENT FUEL IN AN INDEPENDENT SPENT FUEL STORAGE INSTALLATION
- 40 CFR Part 191, ENVIRONMENTAL STANDARDS FOR THE MANAGEMENT AND DISPOSAL OF SPENT NUCLEAR FUEL, HIGH-LEVEL, AND TRANSURANIC RADIOACTIVE WASTES

<u>OCCUPATIONAL SAFETY & HEALTH</u>

- DOE Order 3790.1A, OCCUPATIONAL SAFETY AND HEALTH PROGRAM FOR FEDERAL EMPLOYEES
- DOE Order 5483.1A, OCCUPATIONAL SAFETY AND HEALTH PROGRAM FOR DOE CONTRACTOR EMPLOYEES AT GOVERNMENT-OWNED CONTRACTOR-OPERATED FACILITIES

# REQUIREMENTS (CON'T)

- DOE Order 5480.8, CONTRACTOR OCCUPATIONAL MEDICINE PROGRAM
- DOE Order 5480.9, CONSTRUCTION SAFETY AND HEALTH PROGRAM
- DOE Order 5480.10, CONTRACTOR INDUSTRIAL HYGIENE PROGRAM
- DOE Order 5480.4, ENVIRONMENTAL PROTECTION, SAFETY AND HEALTH PROTECTION

<u>FIRE PROTECTION</u>

- DOE Order 5480.7, FIRE PROTECTION
- DOE Order 5480.4, ENVIRONMENTAL PROTECTION, SAFETY AND HEALTH PROTECTION STANDARDS

# REQUIREMENTS (CON'T)

- 10 CFR Part 60, DISPOSAL OF HIGH-LEVEL RADIOACTIVE WASTES IN GEOLOGIC REPOSITORIES

TRANSPORTATION SAFETY

- DOE Order 5480.3, SAFETY REQUIREMENTS FOR THE PACKAGING AND TRANSPORTATION OF HAZARDOUS MATERIALS, HAZARDOUS SUBSTANCES AND HAZARDOUS WASTES
- 10 CFR Part 71, PACKAGING AND TRANSPORTATION OF RADIOACTIVE MATERIAL
- 49 CFR Part 172, HAZARDOUS MATERIALS TABLES AND HAZARDOUS MATERIALS COMMUNICATIONS REGULATIONS
- 49 CFR Part 173, SHIPPERS - GENERAL REQUIREMENTS FOR SHIPMENTS AND PACKAGINGS

# REQUIREMENTS (CON'T)

- 49 CFR Part 174, CARRIAGE BY RAIL
- 49 CFR Part 176, CARRIAGE BY VESSEL
- 49 CFR Part 177, CARRIAGE BY PUBLIC HIGHWAY

MINING AND DRILLING SAFETY

- DOE Order 5480.4, ENVIRONMENTAL PROTECTION, SAFETY AND HEALTH PROTECTION STANDARDS
- 30 CFR Part 57, SAFETY AND HEALTH STANDARDS - UNDERGROUND METAL AND NONMETAL MINES

# REQUIREMENTS (CON'T)

POSTCLOSURE

- 40 CFR Part 191, ENVIRONMENTAL STANDARDS FOR THE MANAGEMENT AND DISPOSAL OF SPENT NUCLEAR FUEL, HIGH-LEVEL AND TRANSURANIC RADIOACTIVE WASTES

RADIOLOGICAL SAFETY POSTCLOSURE

- 10 CFR Part 60, DISPOSAL OF HIGH-LEVEL RADIOACTIVE WASTES IN GEOLOGIC REPOSITORIES