Advance Diploma in Safety Engineering

Advance Diploma in Safety Engineering

Module 1: Historical and Industrial Perspectives on Safety Engineering

Differences between Workplace Safety and Product/System

Safety A Brief Legal View of the History of Safety

A Technical View of the History of Safety

Workplace Safety Today: An Engineer's View

Product/System Safety Today

- Commercial Aviation
- Nuclear Power
- The Chemical Industry
- Defense and "System Safety"
- SUBSAFE: The US Nuclear Submarine Safety Program
- Astronautics and Space
- Healthcare/Hospital Safety

Summary

Exercises

Module 2: Risk in Modern Society

Changing Attitudes toward Risk

Changing Risk Factors

- The Appearance of New Hazards
- Increasing Complexity
- Increasing Exposure
- Increasing amounts of Energy
- Increasing Automation of Manual Operations
- Increasing Centralization and Scale
- Increasing Pace of Technological Change

How Safe Is Safe Enough?

- Risk-Benefit Analysis and the Alternatives
- Trans-Scientific Questions

Exercises

Module 3: Fundamental Concepts and Definitions

Definitions of Safety and Risk

Hazards and Hazard Analysis

Defining Safety Requirements and Constraints

Safety versus Reliability

What Is a System?

- Assumptions Underlying the Concept of a System
- Sociotechnical Systems

Defining Complexity

Approaches to Dealing with Complexity

- Analytic Decomposition
- Statistics
- Systems Thinking and Systems Theory
- Systems Theory Fundamentals

Summary

Exercises

Module 4: Why Accidents Occur

The Traditional Conception of Causality

Subjectivity in Ascribing Causality

Oversimplification in Determining Causality

- The Legal Approach to Causality
- Human Error as the Cause of Accidents
- Technical Failures as the Cause of Accidents
- Organizational Factors as the Cause of Accidents

Multifactorial Explanations of Accidents

Systemic Causes of Accidents

Social Dynamics and Organizational Culture

- Overconfidence and complacency
- Low priority given to safety
- Flawed resolution of conflicting goals
- Confusing safety with other system properties

Management Decision-Making Structure

- Ill-defined and diffused responsibility, authority, and accountability
- Lack of independence and low-level status of safety personnel
- Limited communication channels and poor information flow

Operational Processes and Practices

- Superficial, isolated, or misdirected safety efforts during operations
- Inadequate feedback and learning from events
- Poorly defined operating procedures
- Inadequate training and emergency management
- Inadequate management of change
- Poor maintenance practices

Government and Professional Society Oversight

Engineering Processes and Practices

- Superficial safety efforts
- Overreliance on redundancy and protection systems
- Ineffective risk control

Safety Information System Deficiencies

Summary

Exercises

Module 5: The Role of Software in Safety

The Use of Software in Systems Today

Understanding the Problem

Why Does Software Present Unique Difficulties?

Software Myths

Why Software Engineering Is Difficult

- Analog versus discrete state systems
- The curse of flexibility
- Complexity and invisible interfaces
- Lack of historical usage information

The Reality We Face

The Way Forward

Exercises

Module 6: The Role of Humans in Safety

Why Replace Humans with Machines?

Do Human Operators Cause Most Accidents?

The Need for Humans in Automated Systems

Human Error as Human-Task Mismatch

- Skill-Based Behavior
- Rule-Based Behavior
- Knowledge-Based Behavior
- The Relationship between Experimentation and Error

The Role of Mental Models in Safety

What Is the Appropriate Role for Humans in Complex Systems?

- The Human as Monitor
- The Human as Backup
- The Human as Partner

Conclusions

Exercises

Module 7: Accident Causality Models

Energy Models

Linear Chain-of-Failure Events Models

- The Domino Model
- The Swiss Cheese Model
- The Functional Resonance Model
- Limitations of Linear Chain-of-Events Models

Epidemiological Models

More Sophisticated Models of Causality

The STAMP Model of Causality

Looking Ahead

Exercises

Module 8: Accident Analysis and Learning from Events

Why Are We Not Learning Enough from Accidents?

- Oversimplification and Root Cause Seduction
- Hindsight Bias
- Misunderstanding the Role of Humans in Accidents
- Focusing on Blame: Blame Is the Enemy of Safety

Goals for Improved Accident Analysis

Example: The Zeebrugge Ferry Accident

Generating Recommendations

Implementing Long-Term Learning

The Cost of Thorough Accident Investigation

Summary

Exercises

Module 9: Hazard Analysis: Basic Concepts

What Is Hazard Analysis?

The Hazard Analysis Process

- The Overall Process
- Detailed Steps

Types of System Models

General Types of Analysis

- Forward and Backward Searches
- Top-Down and Bottom-Up Searches
- Combined Searches

Who Should Do Hazard Analysis?

Limitations and Criticisms of Hazard Analysis

Analysis versus Assessment

Exercises

Module :10 Hazard Analysis Techniques

Energy Model Techniques: Hazard Indices

Techniques Based on the Chain-of-Failure-Events Causality Model

- Failure Modes and Effects Criticality Analysis
- Fault Hazard Analysis
- Fault Tree Analysis
- Event Tree Analysis
- Combinations of Analysis Techniques
- Hazards and Operability Analysis (HAZOP)
- Miscellaneous Techniques

STPA: A Technique Based on STAMP

Task and Human Error Analysis Techniques

- Qualitative Techniques
- Quantitative Techniques

Conclusions

Exercises

Module: 11 Design for Safety

The Design Process

- Standards and Codes of Practice
- Design Guided by Hazard Analysis

Types of Design Techniques and Precedence

Hazard Elimination

- Substitution
- Simplification
- Decoupling
- Elimination of Specific Human Errors
- Reduction of Hazardous Materials or Conditions

Hazard Occurrence Reduction

- Design for Controllability
- Barriers
- Monitoring
- Failure Minimization

Hazard Control

- Limiting Exposure
- Isolation and Containment
- Protection Systems and Fail-Safe Design
- Damage Reduction
- Design Modification and Maintenance

Exercises

Module 12: Human Factors in System Design

Determining What Should Be Automated

The Need for Wide Participation in Design Activities

Safety versus Usability and Other Common Goals

Reducing Safety-Critical Human Errors through System Design

- Safety in the Design of Operator Controls
- Designing Feedback for Safety
- The role of feedback and independent information
- Alarms
- Identifying and Designing the Activities and Functions Provided by Humans
- Combating lack of alertness
- Designing for error tolerance
- Task allocation
- Design of Displays for Safety
- Tailoring the display for human cognitive processing
- Ease of interpretation
- Preparing for failure
- Displaying critical information in a way easy for humans to process
- Feedforward assistance and decision aids

Training and Maintaining Skills

- Teaching about Safety Features
- Training for Emergencies

Exercises

Module 13: Assurance, Assessment, and Certification

Assurance of Safety

Limitations of Traditional Assurance Activities When Used for Safety

Hazard and Risk Assessment

- Qualitative and Quantitative Hazard and Risk Assessment
- Limitations of Hazard and Risk Assessment
- Probabilistic Risk Analysis

Certification

- Types of Certification Approaches
- National and Industry Practices in Certification
- Providing Evidence in Performance-Based Regulation and Safety Cases
- Designing a Certification Program

Some General Conclusions

Exercises

Module 14: Designing a Safety Management System

Social Dynamics and Organizational Culture

- Modeling Desired Behavior
- Documenting Values and Policies

Organizational Structure

- Assigning Responsibility, Authority, and Accountability
- Location of System Safety Activities
- Communication, Coordination, and Information Flow

Management of Safety-Critical System Development

Management of Operational Processes and Practices

- Providing a Shared and Accurate Perception of Risk
- Feedback and Learning from Events
- Creating and Updating Operating Procedures
- Training and Contingency Management
- Managing Change
- Maintenance

Creating an Effective Safety Information System

Summary

Exercises