**Safeware: System Safety and Computers** / Nancy G. Leveson

ISBN-13: 9780201119725

## Table of Contents

I The Nature Of Risk.
Risk In Modern Society.

Changing Attitudes Toward Risk.
Is Increased Concern Justified?.
Unique Risk Factors in Industrialized Society.
Computers And Risk.

The Role of Computers in Accidents.
Software Myths.
Why Software Engineering is hard.
The Reality We Face.
Causes Of Accidents.

The Concept of Causality.
Flaws in the Safety Culture.
Ineffective Organizational Structure.
Ineffective Technical Activities.
Human Error And Risk.

Do Humans Cause Most Accidents?.
The Need for Humans in Automated Systems.
Human Error as Human-Task Mismatch.
Conclusions.
The Role Of Humans In Automated Systems.

Mental Models.
The Human as Monitor.
The Human as Backup.
The Human as Partner.
Conclusions.
II Introduction To System Safety.
Foundations Of System Safety.

Safety Engineering Pre-World War II.
Systems Theory.
Systems Engineering.
Systems Analysis.
Fundamentals Of System Safety.

Historical Development.
Basic Concepts.
Software System Safety.
Cost and Effectiveness of System Safety.
Other Approaches To Safety.

Industrial Safety.
Reliability Engineering.
Application-Specific Approaches to Safety.
III Definitions And Models.
Terminology.

Failure and Error.

Accident and Incident.
Hazard.
Risk.
Safety.
Safety and Security.
Accident And Human Error Models.

Accident Models.
Human Task and Error Models.
Summary.
IV Elements Of A Safeware Program.
Managing Safety.

The Role of General Management.
Place in the Organizational Structure.
Documentation.
The System And Software Safety Process.

The General Tasks.
Conceptual Development.
Design.
Full-Scale Development.
Production and Deployment.
Operation.
>Examples.
Hazard Analysis.

The Hazard Analysis Process.
Types of System Models.
General Types of Analysis.
Limitations and Criticisms of Hazard Analysis.
Hazard Analysis Models And Techniques.

Checklists.
Hazard Indices.
Fault Tree Analysis.
Management Oversight and Risk Tree (MORT) Analysis.
Event Tree Analysis.
Cause-Consequence analysis (CCA).
Hazards and Operability Analysis (HAZOP).
Interface Analyses.
Failure Modes and Effects Analysis (FMEA).
Failure Modes, Effects, and Criticality Analysis (FMECA).
Fault Hazard Analysis (FHA).
State Machine Hazard Analysis (SMHA).
Task and Human Error Analysis Techniques.
Evaluations of Hazard Analysis Techniques.
Software Hazard And Requirements Analysis.

Process Considerations.
Requirements Specification Components.
Completeness in Requirements Specifications.
Completeness Criteria for Requirements Analysis.
Constraint Analysis.
Designing For Safety.

The Design Process.
Design Techniques.
Design Modification and Maintenance.
Design Of The Human-Machine Interface.

General Process Considerations.
Matching Tasks to Human Characteristics.
Reducing Safety-Critical Human Errors.
Providing Appropriate Information and Feedback.
Training and Maintaining Skills.
Guidelines for Safe HMI Design.
Verification Of Safety.

Dynamic Analysis.
Static Analysis.
Independent Verification and Validation.
Summary.
- See more at: http://www.pearsonhighered.com/educator/product/Safeware-System-Safety-and-Computers/9780201119725.page#sthash.tJ1sSiHw.dpuf