SYSTEM SAFETY MANAGEMENT

DR. KAILASH C. KAPUR, P. E.

PROFESSOR

INTRODUCTION

These powerful methods for system safety and reliability which were originally developed and applied in the aerospace and nuclear power industries are increasingly becoming relevant in a variety of business and industrial environments including Department of Defense [DoD]. Continuous changes in technology, environmental regulation, public safety concerns and the need to do more with less all make the analysis of complex systems even more demanding. As the level of uncertainty surrounding probable outcomes increases, the safety and reliability professional's ability to accurately predict responses is integral to the design process for complex systems.

This course covers useful elements, principles, methods and applications for system safety management. System safety/reliability must be integrated into systems engineering, system design, development and testing, and lifelong operational sustainability of DoD equipment. Inductive [FMECA, RBD] and deductive methods [FTA] are covered with examples. Various forms for hazard analysis are discussed. Design for safety and reliability as well as relationships between safety factor and reliability are presented. Concept of risk management is covered as well as its relationship with system safety management.

Course is based on…..

1. Lecture notes prepared by Dr. Kapur over last 40 years
2. Air Force System Safety Handbook
3. MIL-STD-882 [C, D and E,..], DoD Standard Practice for System Safety
4. Fault Tree Handbook with Aerospace Applications- NASA Office of Safety and Mission Assurance, 2002
5. System Safety Management Guide, Department of Army, 385-16
6. ….and many other references.

COURSE TOPICS/CURRICULUM

Overview

The engineering decision processes for complex systems
Foundations and principle-centered philosophy for safety and supportability
Focus on useful and practical approaches with examples and illustrations

Introduction to System Safety

Definitions of System Safety
Traditional Approaches
Standards and Guidance
Management Perspectives
Introductory View of System Safety Objectives

Definitions

The Meaning of Words – Why it Matters!
Mil-Std 882 Definitions
Other Standards – Their Definitions – How They Differ
System Engineering Terms/Definitions
Life Cycle Phases/Definitions

Introduction to Risk

Safety Risk as it Effects Political, Economic, Technical and Social Risks to the Program
Unacceptable, Residual, Acceptable, Unidentified Risk
Safety Versus Risk
Introduction to Risk Management
Responsibilities to Risk (Program Manager, Safety Manager, Engineering Manager etc.)
Introduction to Severity and Probability

Why Safety?

Profit Motive
Legal Vulnerabilities
Social and Humanitarian Attitudes
Directives

System Safety/Reliability Analysis – Basic Intro to Methods

Inductive vs. deductive approaches
Hazard analysis
Criticality and priority matrices
PHA, FMECA, FTA, et al.
Contractual and disciplinary interfaces

Probability Theory and Boolean Algebra

Fundamentals of probability theory
Set theory and Boolean algebra
Applications of Boolean algebra

Safety/Reliability Measures

Measures for safety and reliability
MTBF, percentiles
Failure or hazard rate concept

Statistical Life Distributions

Useful distributions for safety/reliability
Applications and examples

System Reliability/Safety Models

Reliability block diagrams
Models for complex systems
Redundancy
Reliability computations using minimal paths and cuts

Design for Safety/Reliability

Probabilistic design methodology
Safety factor and reliability
Sensitivity analysis

Fault Tree Analysis

Definitions and symbols
Demonstrative vs. investigative models
The analytical process
Guidelines and ground rules

Fault Tree Construction

Introductions to problems
Workshop sessions
Results generalized to illustrate design principles

Inductive Methods

History and applications
RBD
FMECA, FMMECA

Some Useful Statistical Concepts

Estimation using different life distributions
Hypothesis testing and confidence intervals

System Safety Process

Early Assessment of the System/Subsystem Baseline
Definition of Safety Critical Functions
Identification of (early) Generic Safety Requirements/Constraints
Hazard Identification, Documentation, Tracking
System-Level Hazard/Mishap Effects
Categorization of Hazard Risk

System Safety Interfaces with Other Disciplines

Human Factors, Reliability, Maintainability, Supportability, Logistics, and Quality Control
Systems Engineering/Design Engineering/Software Development
Program Management

Human Performance

The Five "P's" (physical, physiological, psychological, psychosocial, and pathological)
Human Performance Capabilities and the Operation Environments

Some Additional Design Considerations

Design for safety and reliability
Single failure systems: active vs. passive components
Sources and treatments of common cause failure

System Safety and Reliability Management

Principles, ideals and applications and illustrations

Background of the Professor

Dr. Kailash [Kal] C. Kapur is a Professor of Industrial & Systems Engineering in the College of Engineering at the University of Washington, Seattle. He was the Director of Industrial Engineering at the University of Washington from January 1993 to September 1999. He was a Professor and the Director of the School of Industrial Engineering, University of Oklahoma from 1989-1992 and a professor in the Department of Industrial and Manufacturing Engineering at Wayne State University, Detroit, Michigan from 1970-1989. Dr. Kapur received the Ph. D. degree (1969) in Industrial Engineering & Operations Research from the University of California, Berkeley, California. He has also had visiting professor appointments at the University of Maryland, College Park; Beijing University of Aeronautics and Astronautics [BUAA], Beijing, China; Norwegian University of Science and Technology, Trondheim and Hong Kong University of Science and Technology, Hong Kong.

He has co-authored the book ***Reliability in Engineering Design***, John Wiley & Sons, 1977. He has co-authored (with Professor Michael Pecht) a new book, ***Reliability Engineering,*** John Wiley, 2014 [to be available in April 2014].He has also published over dozen book chapters in many handbooks such as Industrial Engineering, Mechanical Design, Reliability Engineering and Management, Engineering Statistics, Operations Research and Performability Engineering handbooks. He has published over seventy research papers in scholarly journals and given several keynote speeches at the international conferences in the last couple of years. He received the *Allan Chop Technical Advancement Aw*ard from the Reliability Division and the *Craig Award* from the Automotive Division of American Society for Quality. He is a *Fellow* of American Society for Quality, a fellow of the Institute of Industrial Engineers, and a *registered professional engineer*.