Design for Safety (DfS)

Course Description

Dramatic savings can occur through creative design practices that focus on inherent product risks very early in the design process, and on ways to minimize each risk factor. At a time when safety recalls are becoming an increasingly costly and damaging problem for companies in the automotive and aerospace industries, this seminar reveals how significant cost savings can be obtained by designing for safety.

With a focus on writing clear, accurate safety specifications, attendees will engage in hands-on activities where they will practice balancing intuitive vs. logic-based design considerations. They will also discover risk-mitigation techniques that can be effectively implemented in their workplaces to prevent costly recalls.

Challenging the usual paradigm of "safety costs money," this seminar also explores the creative techniques used by several famous engineering managers to increase safety and decrease costs. Other topics include accident causes and prevention, potential misuse of product, hazard analysis (including latent hazard initiation), testing, and software safety design. A copy of instructor Dev Raheja's text Creativity: The Art of Doing Right Things Right will be provided to each participant.

Overview

By attending this seminar, you will be able to:

- Predict potential accidents before the design is released
- Design creative solutions that reduce costs and deliver higher returns
- Write specifications that clearly define safety requirements and the desired levels of safety
- Identify potential hazards introduced in manufacturing
- Identify safety risks posed by product misuse
- Prepare risk analysis reports for managers to use in decision-making

Intended Audience

This seminar will be especially valuable for:

- Design engineers & managers
- Research & development engineers & managers
- Safety engineers & managers
- Engineers in reliability and quality assurance
- Service engineers & managers
- Any engineer responsible for specification writing
- Any manager responsible for safety, quality or risk management
- Some experience in design will be helpful but not essential

Course Outline

- Safety in Design Concepts
  - System view of safety
  - Boundaries of safety
  - Criteria for safety
- Hands-On Workshop: Safety Boundaries
- Theory of Accidents
  - Domino effect
  - Single causation theory
  - Multiple causation theory
  - Energy control theory
- Writing Safety Specifications
  - Holistic considerations
  - Life cycle considerations
  - Abuse/misuse considerations

  - Robustness criteria for safety
- Hands-On Workshop: Writing Safety Specifications
- Writing Interface Specifications
  - Hardware/software interface
  - Hardware/hardware interface
  - Software/software interface
  - Software/human interface
  - Hardware/human interface
- Safety Design Process to Fine-tune Specifications
  - Hazard analysis
  - Identifying hazards
  - Assessing the risk
  - Mitigating the risk
  - Cost effective control of hazards
- Hands-On Workshop: Hazard Analysis
- Minimizing Accidents in Early Design
  - Conceptual safety analysis
  - Logical solutions
  - Intuitive solutions
  - Innovation with high return on investment
- Minimizing Accidents in Detail Design
  - Subsystem hazard analysis
  - Failure mode, effects, and criticality analysis for safety
  - Fault tree analysis
  - Operations and support hazard analysis
  - Maintenance engineering hazard analysis
- Hands-on Workshop: Safety Enhancement Through Fault Tree Analysis
- Minimizing Accidents in Complex Systems
  - Making use of lessons learned
  - Design for robust human interface
  - Design for robust software interface
  - Design for sneak conditions
- Avoiding Latent Hazard Initiation in Manufacturing
  - Process safety hazard analysis
  - Production qualification for safety
  - Safety inputs to design
  - Design for preventing defects in production
- Hands-on workshop: Designing Out Latent Unsafe Events
- Testing for Safety
  - Prerequisites for developing tests
  - Accelerated testing for safety qualification
  - Safety tests in production and feedback to design
  - Tests for unexpected user related failures
  - Tests for rare events
- Embedded Software Safety
  - Software system safety concepts
  - Requirements analysis for safety
  - Software hazard analysis
  - Identifying new requirements for safety
- Software Safety Design Control Techniques
  - Design control techniques
  - Software preliminary hazard analysis
  - Software failure mode and effects analysis
  - Selecting structure for safety
  - Selecting architecture for safety

About the Instructor

Dev Raheja, the author of Zen and the Art of Breakthrough Quality has over 30 years of hands-on and consulting experience in manufacturing. He served as Manufacturing Engineering Manager at General Electric, Quality Control Manager at Cooper Power Systems, and Senior Reliability and Maintainability consultant at Booz-Allen & Hamilton. He has been a consultant to automotive, medical, and aerospace companies such as GM, Ford, Boeing, Intel, Johnson & Johnson, Mattel, Lockheed, and IBM.

About the Instructor

"Shows safety does not have to cost more. If considered from the beginning, safety can make you money, earn respect, and increase reputation with industry and customers."

Donald R. Phillips
Consulting Engineer
National Forensic Engineers

"Such type of seminars on safety aspects create an awareness in the minds of design engineers from the very early stages."

Pardip Singh
Product Engineer
DaimlerChrysler Corporation