MIL-STD-882E System Safety Course

Outline

- *Introduction*
  - *System Safety*
    - *Overview, Benefits*
    - *What It Is, What It Isn't*
    - *How It Works*
  - *Software Safety*
    - *Overview, Benefits*
  - *Myths*
- *Accidents*
  - *Examples*
  - *Safety Loopholes*
  - *Their Nature & Causes*
- *Simplicity, Determinism*
- *Safety & Reliability Concepts*
  - *Definitions*
- *Designing in Safety*
- *Validating Safety*
  - *Can We Always Validate Safety?*
  - *How Can We Validate Safety?*
    - *When Our System Contains COTS Elements?*
    - *When Little or No Documentation Exists?*
- *Personnel*
  - *Independence*
  - *Credentials*
- *Introduction to Checklists*
- *Risk Concepts*
  - *Definitions*
    - *Severities & Probabilities*
  - *Risk Assessment*
    - *Risk Assessment Matrix/RAC's*
    - *Risk Levels*
  - *Risk Displacement*
  - *882E Risk - Dilemma*
- *Managing Risk*
- *882 Evolution*
- *Overview of 882E*
  - *100 Series Tasks*
  - *200 Series Tasks*
  - *300 Series Tasks*
  - *400 Series Tasks*
  - *Changes, Additions, More Dilemmas*
  - *Surprises, Confusion*
- *Other Useful System Safety Standards & Guidelines*
- *Safe Design Techniques*
- *Requirements Checklist*
- *Design Checklist*
- *System Safety Programs (SSP)*
  - *Objectives*
  - *General Requirements*
  - *Tailoring*
  - *Flow-Down of Safety Requirements*
  - *Safety Integration*
  - *Safety Requirements Traceability*
    - *Tools*
  - *Design/Implementation/Testing Influence*
  - *Chronology*
  - *Safety Program Results*
  - *How to Properly Orchestrate an SSP*
    - *With or Without Subcontractors*
  - *Links to Software Safety*
- *Safety Management Plans (SMP)*
- *System Safety Program Plans (SSPP)*
  - *Very In-Depth*
- *System Safety Working Groups (SSWG)*
- *Safety Assurance Concepts (SACs)*
- *Hazard Mitigation Precedence*
- *Hazard Tracking*
  - *Hazard Logs & Their Design*
  - *Wrinkles In 882E*
- *Preliminary Hazard List (PHL)*
  - *Overview, Guidelines, Example*
  - *Class Assignment*
- *Preliminary Hazard Analysis (PHA)*
  - *Overview, Pitfalls*
  - *Formats*
  - *Guidelines - Keys to Success*
  - *Example, Class Exercise*
- *Subsystem Hazard Analysis (SSHA)*
  - *Overview, Difficulties, Guidelines*
- *System Hazard Analysis (SHA)*
  - *Overview, Guidelines*
- *Operating & Support Hazard Analysis (O&SHA)*
  - *Very In-Depth*
- *Human Factors*
  - *EOO, EOC, CTE*
  - *Human Reliability Analysis*
  - *Integrating HF and System Safety*
- *Health Hazard Analysis (HHA)*
  - *Detailed Description*
- *Functional Hazard Analysis (FHA)*
  - *Read Between The Lines!*
- *Systems of Systems (SoS) Hazard Analysis*
- *Safety Assessment Reports (SAR)*
  - *Overview, Example*
- *Change Analysis*
  - *Analyzing ECPs, RFDs, RFWs*
- *FMEA*
  - *Getting It Wrong*
  - *Examples, Guidelines*

- *FMECA*
  - *Criticality Analysis*
  - *RPN/CI*
  - *Examples*
- *Fault Tree Analysis (FTA)*
  - *Qualitative/Quantitative*
  - *Versus FMEA/FMECA*
  - *Advantages/Disadvantages*
  - *Fault Tree Symbols and Terminology*
    - *Definitions, Special Symbols*
  - *Examples*
  - *Immediate, Necessary and Sufficient Concept*
  - *Basic Rules*
  - *System Operational Modes*
  - *Guidelines - Keys to Success*
    - *Increased Accuracy, Consistency, Economy*
    - *Best Kept Secrets?*
  - *Maintainability*
  - *Fault Tree Notes*
  - *Step Size Precautions*
  - *Similar Subtrees*
    - *Limiting Fault Tree Size, Sharing Subtrees*
  - *Improving Consistency*
  - *Fault Tree Reviews*
  - *Design/Implementation Influence*
  - *Cut Sets, Minimal Cut Sets*
  - *Minimal Cut Set Analysis*
    - *What This Really Means*
  - *Common Mode Analysis*
  - *Acceptance/Rejection Criteria*
    - *28 Attributes*
  - *Limiting Fault Tree Production*
  - *Class Exercise – Introductory*
  - *Class Exercise – More Difficult*
  - *Fault Tree Analysis Programs*
- *Software Safety*
  - *Overview*
  - *Standards & Guidelines*
    - *JSSSEH*
    - *AMCOM 385-17*
      - *Origins with HCRQ*
    - *et al*
  - *Software Safety Criticality*
    - *Software Control Categories*
    - *Software Safety Criticality Matrix/SwCI's*
  - *Approaches*
  - *Software FMEA*
  - *Software FMECA*
  - *Software FTA*
- *Dealing with COTS Elements*
- *Avoiding the Money Pit*
- *Safety Compliance*
- *Safety Verification*
  - *Testing*
- *Safety Audits*

Covered In Appendices

Secondary Definitions
Safety Conferences/Associations/News Groups
Much More

HCRQ, Inc.
7151 Richmond Road, Suite 201
Williamsburg, VA 23188
Tel: (757) 564-7703
Fax: (757) 564-7704

web: http://www.hcrq.com/Training.html
e-mail: training@hcrq.com