



System Safety

-

5-Day 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 & Cause

Simplicity, Determinism

Safety & Reliability Concepts

Definitions

Generic Integrity Levels

System, Software

Safety Integrity

Systematic & Random Failure Integrity

Levels

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?

Reliability Allocation & Prediction

Personnel

Independence

Credentials

Introduction to Checklists

Risk Concepts

Definitions

Hazard Severities & Probabilities

Defined by Standards

ALARP

System Hazard Risk Assessment

Hazard Risk Assessment Matrix/HRI's

MIL-STD-882

Other Examples

Risk Classes

Safety Integrity Level Determination

System, Software

Risk Displacement

Managing Risk

Socioeconomic Factors

System Safety Standards & Guidelines

MIL-STD-882

Introduction

MIL-STD-882B

MIL-STD-882C

MIL-STD-882D

MIL-STD-882E (pending)

Differences, Strengths, Weaknesses

Army Reg. 385-16

GEIA-STD-0010

Overview

Peculiarities

SAE ARP4754, 4761

Introduction

4761 Compared to 882

Peculiarities

RTCA DO-178B, 254

The Level Dilemma

DEF STAN 00-56

Introduction

Comparison With 882

Peculiarities

The ISA Dilemma

IEC 61508

Introduction

Peculiarities

Other System Safety Standards, Guidelines

EN 50126, EN 50129

Air Force System Safety Handbook

FAA System Safety Handbook

et al

Safe Design Techniques

Requirements Checklist

Design Checklist

System Safety Management

System Safety Management Plans (SSMP)

Content

Corporate Safety Policy

Corporate Environmental Policy

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

System Safety Program Plans (SSPP)

Very In-Depth

System Safety Working Groups (SSWG)

Hazard Mitigation Precedence
Hazard Tracking
 Hazard Logs & Their Design
Preliminary Hazard List (PHL)
 Overview, Guidelines, Example
 Class Assignment
Preliminary Hazard Analysis (PHA)
 Overview, Pitfalls
 Formats
 Guidelines - Keys to Success
 Example, Class Exercise
Safety Requirements/Criteria Analysis
Subsystem Hazard Analysis (SSHA)
 Overview, Difficulties, Guidelines
System Hazard Analysis (SHA)
 Overview, Guidelines
Safety Assessment Reports (SAR)
 Overview, Example
Operating & Support Hazard Analysis (O&SHA)
 Overview, Guidelines, Example
OSHA
 Job Hazard Analysis
Change Analysis
 Analyzing ECPs, RFDs, RFWs
Human Factors
 Role
 Interfacing HFE and System Safety
Human Reliability Analysis (HRA)
Health Hazard Assessment (HHA)
 Detailed Description
Failure Conditions
 Classifying
 Quantitative Targets
 Qualitative Targets
 Development Assurance Levels
 What?
 System, Item, Software, Hardware
 Derivation, Rules
Function Hazard Assessment (FHA)
 Description
 Aircraft Level
 Example
 System Level
 Example
Preliminary System Safety Assessment (PSSA)
 Description
 Example
System Safety Assessment (SSA)
 Description
 Example
Common Cause Analysis (CCA)

Zonal Safety Analysis (ZSA)
Particular Risks Analysis (PRA)
Common Mode Analysis (CMA)
FMEA
 Examples, Guidelines
 Class Exercise
FMES
FMECA
 Criticality Analysis
 RPN/CI
 Examples
Other Techniques
 HAZOP Studies
 What-If Analysis
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
 20 Attributes
 Limiting Fault Tree Production
 Class Exercise – Introductory
 Class Exercise – More Difficult
 Fault Tree Analysis Programs
System Safety Case
 Introduction
 Goal Structuring Notation (GSN)
 Preparation
 Guidelines
Software Safety - In-depth

Standards & Guidelines
 IEEE 1228
 AMCOM 385-17
 JSSSEH
 AOP-52
 EN 50128
 NASA
 et al
Software Safety Program Plan
Software Hazard Risk Assessment
 Software Control Categories
 Software Hazard Criticality Matrix/SHRI's
 Software Levels
 DALs, SILs
Approaches
 Software FMEA
 Software FMECA
 Software FTA
 Software Safety Cases
Dealing with COTS Elements
Avoiding the Money Pit
Safety Compliance
Safety Verification
 Testing
Safety Audits

Covered In Appendices

Safety Conferences/Associations/News Groups
Petri Net Analysis
Ishikawa Diagrams
Event Tree Analysis
Reliability Block Diagrams
Importance Analysis
Sneak Circuit Analysis (SCA)

HCRQ, Inc.
P.O. Box 264
Williamsburg, VA 23187
Tel: (757) 564-7703
Fax: (757) 564-7704

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