



# Aviation System

## Safety Course

### Outline

---

#### Introduction

##### System Safety

Overview, Benefits

What It Is, What It Isn't

How It Works

##### Software Safety

Overview, Benefits

What It Is, What It Isn't

How It Works

##### Myths

##### Accidents

Examples

Safety Loopholes

Their Nature & Cause

##### 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

Hazard Severities & Probabilities

System Hazard Risk Assessment

Hazard Risk Assessment Matrix/RAC's

Risk Displacement

##### Managing Risk

##### Failure Conditions

Classifying

Quantitative Targets

Qualitative Targets

Development Assurance Levels

What?

System, Item, Software, Hardware

Derivation, Rules

##### System Safety Management Plans (SSMP)

In-Depth Coverage

##### 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)

In-Depth Coverage

System Safety Working Groups (SSWG)

Hazard Mitigation Precedence

Hazard Tracking

Hazard Logs & Their Design

SAE ARP4754A, 4761, RTCA DO-178B, 254

Overview

What's Missing?

Function Hazard Assessment (FHA)

Detailed Description

Aircraft Level

Example

System Level

Example

Preliminary System Safety Assessment (PSSA)

Detailed Description

Example

System Safety Assessment (SSA)

Detailed Description

Example

RTCA DO-178B

Overview

Versus Software Safety

RTCA DO-254

Overview

Common Cause Analysis (CCA)

Zonal Safety Analysis (ZSA)

Particular Risks Analysis (PRA)

Common Mode Analysis (CMA)

Certification Maintenance Requirements (CMR)

Introduction

Safety Assessment Implications

Minimum Equipment List (MEL)

Introduction

Safety Assessment Implications

Preliminary Hazard List (PHL)

Preliminary Hazard Analysis (PHA)

Coverage/Depth Based on Audience Interest

Subsystem Hazard Analysis (SSHA)

Coverage/Depth Based on Audience Interest

System Hazard Analysis (SHA)

Coverage/Depth Based on Audience Interest

Operating & Support Hazard Analysis (O&SHA)

*Overview, Guidelines, Example*  
*Human Factors*  
*Role*  
*Interfacing HFE and System Safety*  
*Change Analysis*  
*Analyzing ECPs, RFDs, RFWs*  
*Safety Assessment Reports (SARs)*  
*In-Depth Coverage*  
*Step Aside FAA DID!*  
*Safe Design Techniques*  
*Requirements Checklist*  
*Design Checklist*  
*FMEA*  
*Examples, Guidelines*  
*Class Exercise*  
*FMES*  
*FMECA*  
*Criticality Analysis*  
*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*  
*Acceptance/Rejection Criteria*  
*20 Attributes*  
*Limiting Fault Tree Production*  
*Class Exercise*  
*Fault Tree Analysis Programs*  
*Dealing with COTS Elements*  
*Safety Compliance*  
*Safety Verification*

*Testing*  
*Safety Audits*

**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](mailto:training@hcrq.com)**