Software System Safety Course

The Software System Safety training course is an integrated combination of system safety, software safety, and software engineering technology. It is designed for safety professionals wanting to advance their skill and knowledge in techniques of software system safety.

To set the stage for the Software System Safety (SwSS) process, the course provides an introduction and review of Risk Management, System Safety, and Software Development. The course provides details of the SwSS process, beginning with a discussion of the importance of integrating SwSS activities into the System Safety Program, the Software Development activities and Systems Engineering activities. The relationship of the Software Hazard Criticality Matrix (SHCM) and Level of Rigor (LOR) to the overall System Safety effort is included, as well as the importance of identification and tracking of safety-critical requirements. Specific analyses and evaluation tools are discussed and illustrated by examples. Details of the SwSS process are discussed for each of the Software Development phases: 1) concept refinement, 2) requirements and architecture development, 3) design and coding, 4) test, validation, and verification, and 5) software release (delivery). Each of the modules is listed below with representative examples described on the reverse of this sheet:

- Course Introduction
- Concepts in Risk Management
- Principles of System Safety
- Initiating a System/Software Safety Program
- Hazard Analysis
- Human Factors
- Software Development Overview
- Intro to Software System Safety
- Software Assurance/Integrity
- Software System Safety Analyses
- Software Safety Process
- Software System Safety Technical Reviews
- Airworthiness
- Lessons Learned

Course Duration and Format
The course is 24 hours over 3 days, with about 6 hours of lecture each day and time for students to complete workshop problems or review course materials with the instructor. Class size will be limited to 30 attendees. Attendees of this course will be credited with 2.4 Continuing Education Units (CEU) upon completion of the course.

Safety Engineering and Analysis Center
The APT Safety Engineering and Analysis Center (SEAC) is conveniently located in Cummings’ Research Park near Redstone Arsenal in Huntsville, AL.
Software System Safety Process Overview

1 System Concept Refinement Phase - Identify

- Assess the user needs, system capabilities, etc.
- Develop safety management documentation
- Assess system and SW development structure and processes
- ID resources req’d, SOW and RFP inputs
- Tailor the SS and SwSS programs
- Integrate SwSS processes within the SW development (SDP, SDD, SEP)
- Initiate hazard analysis activities

2 Software Requirements and Architecture Development Phase – Identify & Assess

- Identify System Hazards and SCSFs
  - Identify and track system level hazards
  - Identify SCSFs based upon functional allocation of system
  - Identify SW contributions to identified system hazards
  - Identify software safety requirements based upon SCSFs
  - Identify SD safety design requirements based upon SD process and guidance documentation (JSSSH, STANAG 4404)
  - Perform software criticality analysis
  - Support Configuration Control Process

3 Software Design & Code Phase

- Execute the SwSS Program. Mitigate SW Hazard Causes
  - Contribute to detailed SS analyses
  - Update detailed SwSS analyses
  - Refine SCSFs
  - Derive any additional lower level software safety requirements
  - Determine verification methods for safety requirements
  - Ensure and track integration of software control measures
  - Perform Level of Rigor Analysis
  - Assess effectiveness of software hazard controls

4 Software Test, Verification & Validation

- Monitor Test, Verification, and Validation
  - Ensure unit, system and integration test plans address SW safety Level of Rigor
  - Support development of safety specific test cases
  - Monitor test and verification activities
  - Review results of test and verification activities
  - Ensure test failures related to safety are documented, corrective actions identified and implemented, and regression testing performed
  - Update requirements tracking database and hazard tracking logs to reflect validated requirements

5 Software Release & Delivery

- Support Software Release/Assess Hazard Risk /Track Risks to Acceptance
  - Monitor software release process
  - Review system level hazards, controls and verifications
  - Assess adequacy and independence of hazard controls
  - Determination of formal final and/or residual risk
  - Support development of SSRAs for residual risks
  - Prepare for Technical Reviews and SW (Material) Release
  - Evaluate software issues and resolutions after fielding

APT Point of Contact
Megan Stroud
256.327.3373
training@apt-research.com