

SOFTWARE SYSTEM SAFETY ENGINEERING

Training offered by A-P-T Research, Inc.

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

The course describes generic SwSS processes adaptable to a variety of customer needs, and is tailorable to specific projects and software development processes. Each course module contains material designed to provide the student with the information and detail needed to understand and apply the material. The course is constantly updated to include new techniques, in-depth processes, and real-life examples. Exercises and quizzes are included to build student confidence when applying software system safety principles.

The SwSS course begins with an overview of course objectives, the need for SwSS, and a description of the relationship between system safety and SwSS. After a discussion of directives, documents, policies and regulations related to SwSS, the course provides detailed instruction on the SwSS process, including a variety of analyses and tools. The instruction concludes with planning details for a SwSS program, hazard identification and tracking, risk assessment, risk reduction, and risk acceptance as applicable to SwSS. In keeping with APT's commitment to excellence, recent updates to the course include modules titled "Programmable Logic Devices," "Model-Based Software Safety," and "The Future of Software System Safety."

An overview of APT's SwSS Process is depicted on the reverse of this sheet.



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 typically be awarded up to 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.

Where

The A-P-T Research, Inc. Safety Engineering and Analysis Center in Huntsville, AL or customer location as requested.

Schedule & Cost

Offered on a regular basis. Visit www.apr-research.com/training for specific dates and prices.

Contact Information

Megan Stroud
256.327.3373
training@apr-research.com

Other Courses Available

- System Safety Engineering
- Explosives Safety
- Managing Risk for Multiple Disciplines
- Reliability Engineering
- IMESAFR Software
- SAFER Software
- Counter-IED Training & Training Devices

For information on other training classes offered by APT, visit www.apr-research.com/training.

It is the policy of A-P-T Research, Inc. that those leading a learning event (instructors, guest lectures, etc.) disclose proprietary interest in any products, services, instruments, devices or materials discussed during a learning event. This includes any source of third-party compensation. Leaders of a learning event are required to disclose this information in the form of a verbal announcement at the beginning of the learning event.

Software System Safety Process Overview

1 System Concept Refinement Phase - Identify

Program Initiation/Safety Planning/System Assessment

- 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

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

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

Iteration & Feedback

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 verified requirements

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

APT Point of Contact

Megan Stroud
256.327.3373
training@apt-research.com



A-P-T RESEARCH, INC.

4950 Research Drive
Huntsville, AL 35805
www.apt-research.com