A-P-T RESEARCH, INC.

SOFTWARE SYSTEM SAFETY

Optimizing Safety Throughout all Phases of the System

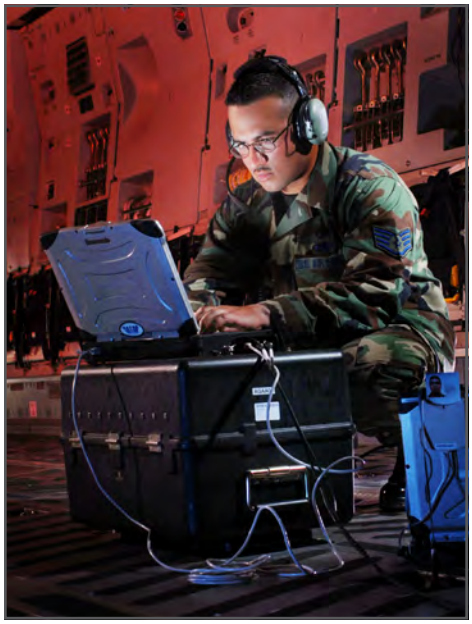
Software System Safety (SwSS) is the application of rigorous methods and analyses to the software that controls or contributes to system hazards. It typically requires application of system engineering, software engineering, and safety engineering principles, and brings the different engineering disciplines together to focus on how software affects the safety of the system. Software System Safety defines the safety requirements for software developers and assures the application of the required level-of-rigor to implementation and compliance with those requirements.

APT's Software System Safety Process

A proven software safety program, this process is successfully applied to major DoD programs. APT supports customers with AMCOM Regulation 385-17 compliance and presentation to the Software System Safety Technical Review Panel (SSSTRP) for software fielding approval. This process includes the following steps:

Process Steps

1. Safety Program Initiation, System Assessment, Safety Planning
2. Identify System Hazards, Identify Software Functions (or Safety-Significant Software Functions)
3. Execute the SwSS Program, Mitigate Software Hazard Causes
4. Monitor Test, Verification & Validation
5. Support Software/ Materiel Release, Assess Hazard Risk, Track Risks to Acceptance



Accomplishments

- Providing software airworthiness input to MIL-HDBK-516 updates
- Developed system safety management plans, system safety program plans
- Identified safety critical software functions and requirements
- Performed independent software safety assessments
- Performed/analyzed hazard tracking data
- Performed software safety analyses
- Prepared software safety metrics plan
- Implemented software safety metrics program

Capabilities

- Plan/implement software system safety programs
- Perform and evaluate hazard analyses
- Secretariat for software system safety working groups
- Perform independent software safety assessments
- Plan/implement software safety metrics program
- Conduct software system safety training

Customers

- Integrated Air & Missile Defense (IAMD)
- AMRDEC-SED
- Textron
- United Space Alliance
- Lockheed Martin
- Missile Defense Agency
- iRobot
- Oshkosh Defense
- Hydroid/Kongsberg

Programs

- M299 Launcher
- Hellfire
- Griffin™
- UAS Universal Ground Control System
- UAS Ground Based Sense and Avoid System
- NLOS-LS
- WAH-64
- Gladiator UGV
- ABV UGV
- CH-47
- JLENS Aerostat
- Sentinel
- FCS UAS
- JBC-P
- JLTV
- FMTV

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 required, SOW and RFP inputs
- Tailor the SS and SwSS programs, document in SSMP, SSPP, and SwSSPP
- Integrate SwSS processes within the SW development (SDP, SDD, SEP)
- Initiate hazard analysis activities

2 Software Requirements & Architecture Development Phase – Identify & Assess

Identify System Hazards and Safety-Significant Software Functions (SSSFs)

- Identify and track system level hazards
- Identify SSSFs based upon functional allocation of system
- Identify SW contributions to identified system hazards
- Identify software safety requirements based upon SwSFs
- 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 system safety analyses
- Update detailed SwSS analyses
- Refine SwSFs
- 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 verified 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 risks
- Support development of SSRAs for residual risks
- Prepare for Technical Reviews and SW (Materiel) Release
- Evaluate software issues and resolutions after fielding

Iteration & Feedback

APT Point of Contact

Rhonda Barnes
256.327.3373
aptinfo@apt-research.com

A-P-T RESEARCH, INC.

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

M-09-00808