

SOFTWARE SYSTEM SAFETY

Optimizing Safety Throughout all Phases of the System

Software System Safety is the application of rigorous methods and analyses to the software that controls hardware 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 implementation and compliance with those requirements.

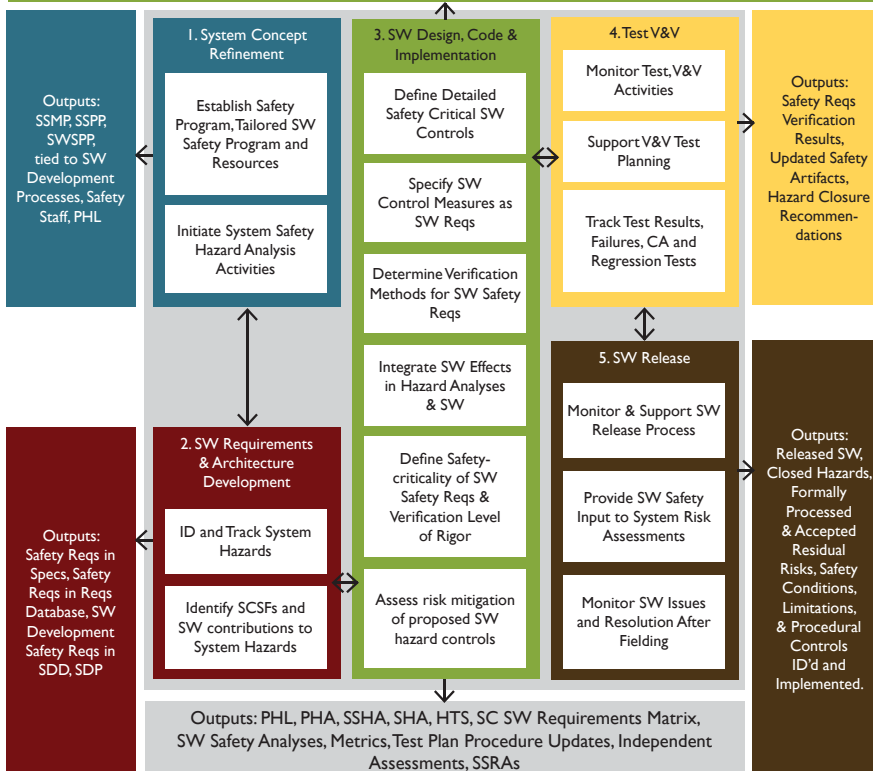
APT's Software System Safety Process

A proven Software Safety Program. This process has been successfully applied to major DoD programs and is currently implemented on the Ground-Based Mid-course Defense (GMD) program. This process includes the following steps:

1. System Concept Refinement Phase – Identify
2. Software Requirements and Architecture Development Phase – Identify & Assess
3. Software Design, Code, and Implementation Phase
4. Software Test, Verification, and Validation Phase
5. Software Release Phase

Team: Program Management, System Engineering, System Safety, SW Safety, SW Developers, SW Testers, V&V, SW Quality Assurance, Configuration Management, User

Outputs: Detailed SW Safety Analyses (FTA, SW SRCA, SSHA, SHA, etc.), Detailed SW Control Measures Specified in SRSs, Verification Methods and Level of Rigor Requirements Defined for SW Safety Requirements, Updated Requirements, Database with Safety Criticality and Level of Rigor, SW Code with Implemented Safety Requirements, Traceability, Evidence – System-Hazards-Requirements-SW Design-SW Code, Updated System Safety Artifacts Incorporating SW Safety Analyses and Results



Satisfies System Safety requirement for a structured safety process that Identifies, Assesses, Reduces the Risk of, and Assesses/Accepts the Residual Risks of the Software's contribution to System Hazards

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

- Lockheed
- iRobot
- AMRDEC-SED
 - NLOS-LS
 - WAH-64
 - Gladiator
 - ABV
 - CH-47
 - Kiowa Warrior
 - JLENS
 - FCS UAS
- Textron
- United Space Alliance

Accomplishments

- Identified safety critical software functions & requirements
- Performed independent software safety assessments
- Performed/analyzed hazard tracking data
- Performed software safety analyzes
- Prepared software safety metrics plan
- Implemented software safety metrics program



APT Point of Contact

Rhonda Barnes
256.327.4006
Rhonda.Barnes1@us.army.mil

Ms. Barnes has over 25 years of diverse experience in the software engineering and simulation industries with emphasis on management (both technical and executive).



A-P-T Research, Inc.

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