APT's Tailorable Software Safety Process

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 the SSMP, SSPP, and SWSSPP
- 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 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 SS 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