Safety Assessment Workshop
Bled – 21st of September 2011

David Morton

SPS Safety & Quality Manager

Overview of ARTAS

- Late 1980's – Early 90's
  - Prototyping and 1st ARTAS Version 1
- Early 90's - Year 2001
  - Development & Maintenance conducted by Thales ATM
  - Mil 2167A Standard used
  - Full and complete development process was applied
  - ARTAS versions covered during this period were V1 – V6B2
- 2001
  - New Industrial Partner (COMSOFT) to carry out Development & Maintenance
  - New Centralised ARTAS Maintenance And Support team (CAMOS) establish to provide services to Users

Overview of ARTAS - Continue

- 2006 - 2008
  - An ARTAS V7 Safety Assessment Study was conducted by CSE Ltd to assess what actions need to take place to allow ARTAS to reach SWAL3 compliance.
  - Identified or reaffirmed those areas where ARTAS is either compliant or more importantly, those areas for which further evidence was necessary to achieve SWAL3.
- ARTAS chose the Eurocontrol Recommendations for A.N.S Software. Ref: SAF.ET1.ST03.1000-GUI-01-01 as the reference document for Safety objective for SWAL3 compliance.

Overview of ARTAS - Continue

- *Areas of improvement:*
  - Provide complete traceability between ARTAS requirement specifications, design and testing.
  - Fully Test all ARTAS requirements at System and/or Software Level.
  - Re-establish a complete set of Architectural Design Documents
  - Need to redesign the Man Machine Interface CSCI

Note: From this point onwards our industrial Partners and Eurocontrol became committed to develop and maintain ARTAS as a SWAL3 compliant system.

Safety Activities

- Documentation:
  - *Actions*
    - Project was created to transfer all Requirement Specifications into a documentation Traceability tool. i.e. DOORS
    - Documentation was structured into DOORS modules to mirror the existing documentation V lifecycle model used for ARTAS. i.e. URD, SSS, SRS, SDD through to testing
    - Provide requirement traceability between each level of documentation.
  - *Findings:*
    - Produced an extremely complex documentation environment which requires dedicated resource.
    - Did however identify:
      - Traceability Gaps between existing requirement
      - Correctness of existing requirement traceability
      - Put into question validity of existing requirements and whether some were indeed testable.

Safety Activities

- *Consequence*
  - Creation of Requirement Writing Guidelines to ensure:
    - a one “shall” requirement
    - requirement is worded correctly to ensure it is testable …..
  - Creation of Requirement Naming Conventions to ensure:
    - Uniqueness for requirement identification
  - Creation of a Documentation Change Notice Template:
    - Provide guidance as to structure and format documentation changes should be written to assist entry into DOORS environment e.g. Safety, Historical data Attributes.

Safety Activities

- Testing
  - *Actions*
    - Test Battery Projects were created to provide one or more tests for each ARTAS CSCI Requirement.

Note: A decision was taken within the ARTAS Product team that System requirements can be covered by 1 or more CSCI requirement test. If however this is not the case, System testing shall be necessary to ensure full coverage.

    - 2 Test Battery projects were created:
      - TRK CSCI + TRK IIRS Requirement Testing
      - SRV & RBR CSCI + IIRS Requirement Testing
  - *Findings:*
    - Need to ensure that where ever possible testing should be automated
    - The use of an automated test tool would be required to run a substantial number of tests being generated.

Safety Activities

- *Consequence*
  - Creation of Test Description & Test Report Templates
    - Provide means to provide standard input of test description information and test data i.e. scenario, database names, test scripts etc..
    - Ensure traceability between Requirement ID, Test Description ID and Test Report ID
    - Enable traceability to requirements within DOORS

Safety Activities

- Architectural Design

  - *Actions*
    - SDD Projects were created a full set of design documents at Architectural Design Level based on latest ARTAS software
    - Reverse engineered source code using Rhapsody design tool in conjunction with DOORS to produce export MS Word documents
    - Enable design components (CSC) to be traced to Software Requirements

  - *Findings:*
    - Unable to fully automate documentation production therefore some manual intervention is necessary
    - Using the reverse engineering process with the source code to generate the design model has led to their production being carried out at the end of the development lifecycle i.e. Once the normal yearly FAT has been concluded and the FATéd code is made available.

Safety Activities

- *Consequence*
  - Limited disruption foreseen as likelihood of a design change occurring the yearly development cycle is seen as minimal
  - All ARTAS Change Proposals and Trouble Reports shall be monitored for any alteration to the design.
  - To ensure any design change is recorded as early as possible, all change shall be recorded using the documentation change notice. i.e. New requirement, additional components at CSC level, traceability between both etc.

Recording SWAL 3 compliance evidence

- The Recommendations for A.N.S Software document does provide an example of a Software Safety Folder template for use to record Safety Evidence.
- ARTAS has chosen to use the DOORS traceability tool to produce a SSF Report by way of creating for each SWAL3 Objective:
  - A unique objective ID with the following attributes
    - Objective Title
    - Objective Description
    - SWAL Compliance Level to be achieved
    - Current status
    - Location of Evidence (specific pathname provided)

  What type of evidence shall be recorded:

SWAL3 Evidence

- Current Documentary evidence includes:
  - System & Software Documentation: SSS, SRS, SUM, etc.
  - Test documentation: e.g. System, Pre-FAT and FAT Plans, Description, Scripts & Reports, Release Notes, VCRI, MCL.
  - User Documentation: e.g. AOH, Installation Manual, CSCI Parameter documents.
  - ARTAS Project documentation: e.g. PMP, QMP, CMP, SAP.
  - ARTAS Development Documentation: e.g. SVVP, SDP.
  - Standards, Procedures, Rules, Guidelines & Methodologies
  - Safety ATR/ACP Safety and Quality Lifecycle Checklists & FAT Safety Reports from ARTAS V7A1 PS2 onwards.
  - Safety Documentation: e.g. Independent Safety Assessment Reports, New SWAL3 projects: e.g. FHA, PSSA Reports
- +……All evidence to support each and every SWAL 3 Objective as and when it becomes available .

Suggestions to reach your desired Software Assurance Level

- Ensure you select a Assurance Level that best suits your needs:
  - Consult the S/W Lifecycle document (ANS Software Lifecycle SAF-ET1-ST03-1000-REP-01-00- V3.0) that provides guidance material for defining an ANS software lifecycle.
  - It also provides references to five existing standards (ED109, IEC12207, IEC61508, ED12B/DO178B and CMMi) and how these standards cover ANS needs.
- To achieve any Software Assurance Level requires resource, time and that dreaded word “Finance”. One needs full commitment from Management for all three.
- Never stop questioning the process and methods used for developing and maintaining the system. Continuous improvement to daily activities should be sought. Automate or streamline process were ever possible. Make thing more efficient.
- Reaching a Software Assurance Level comes about to a large extent by following good software development lifecycles, processes and procedures. i.e. If Industry provide high quality software then a large part of our work by default is done.
- Work closely together with your industrial partners to establish a good understanding of what your expectation are and what level of quality they can provide.

Thank you for listening

Any Questions?