Astrium Satellites generic functional avionics Verification and Validation approach

Michel JANVIER,

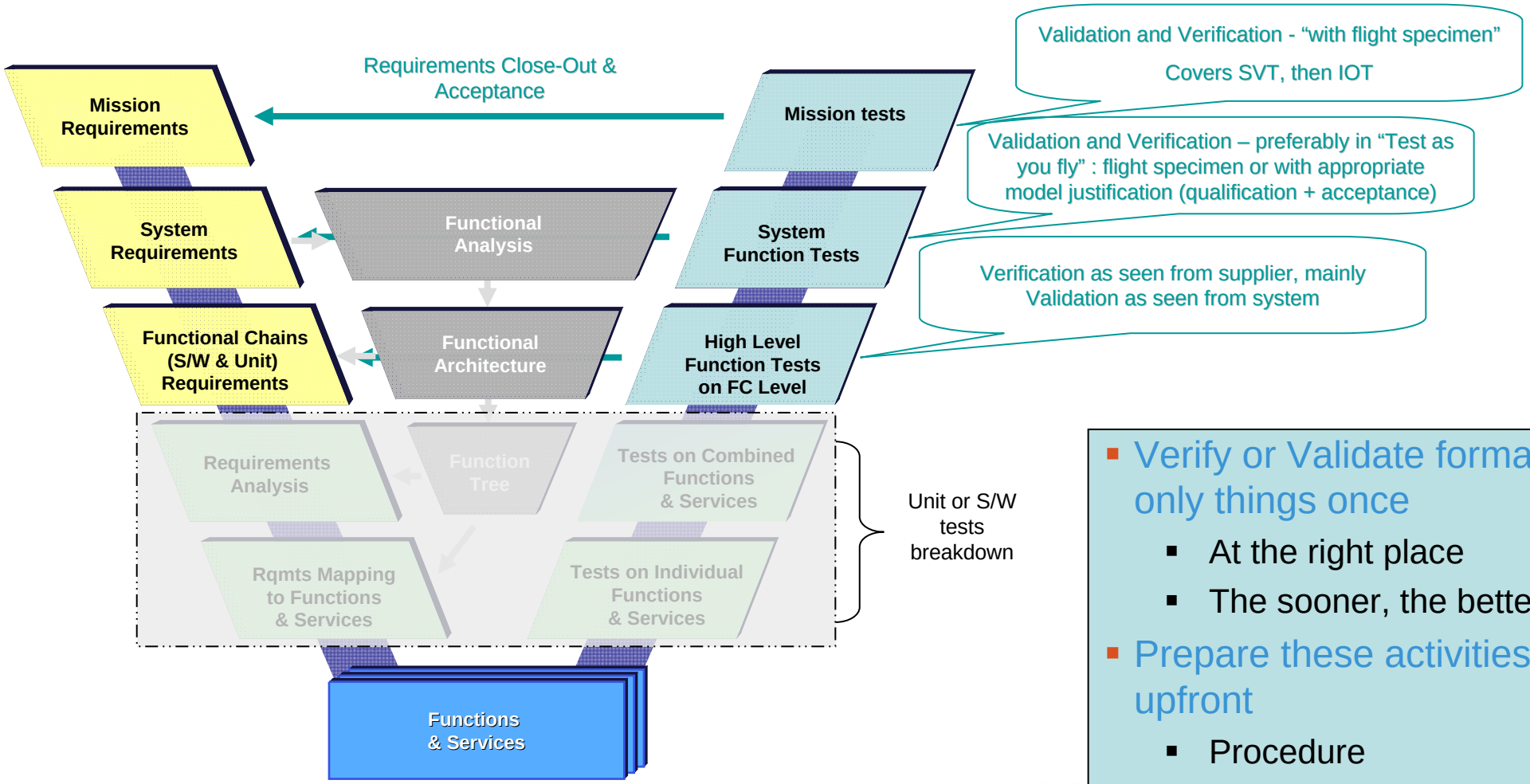
Earth observation Navigation and Science Functional Verification MPC manager

Astrium Satellites (AET2), 26/10/2011

All the space you need

ASTRIUM
AN EADS COMPANY

The Avionics Verification & Validation cycle



- Verify or Validate formally only things once
  - At the right place
  - The sooner, the better
- Prepare these activities upfront
  - Procedure
  - Benches

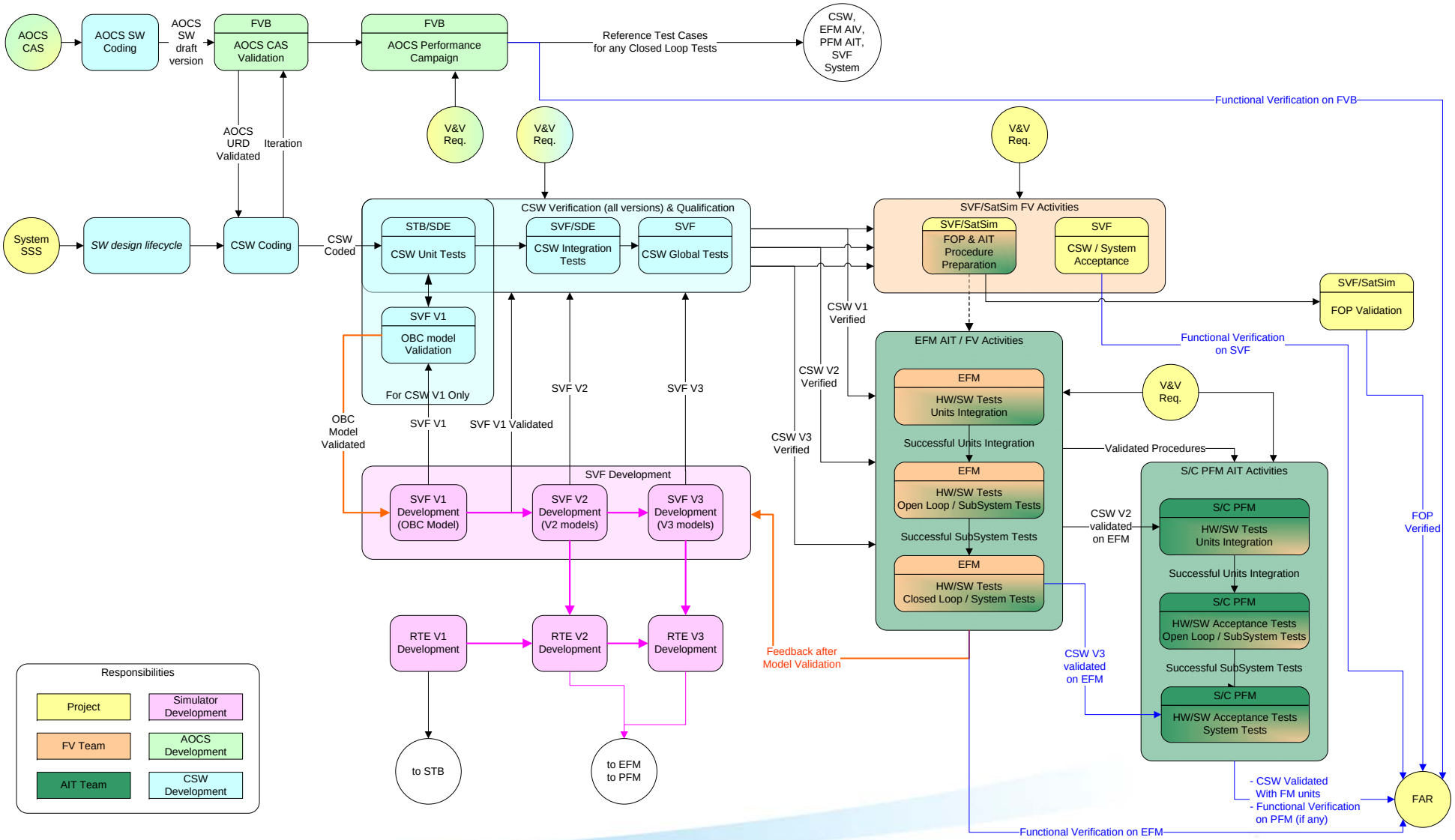
Test Bench Definitions / Objectives

"Design Environments & Numerical Benches"	
SDE S/W Development Environment	To develop the on-board software and perform the tests on module / unit level based on standard facilities of the internal software development team or external supplier. *(Tests on Individual Functions& Services)*
OSE (AOCS) Offline Simulation Environment	To support the AOCS algorithm design (CAS), based on a functional simulation of environment, dynamics and sensors and actuators. *(ECSS-E-TM-10-21A class : Functional Engineering Simulator)*
FVB (AOCS) Functional Validation Bench	To support the development, verify and validate AOCS algorithms and performance, allowing closed loop simulations with either an image of the AOCS flight S/W application or single modules of the AOCS flight S/W in the loop. *(ECSS-E-TM-10-21A class : Functional Validation Test bench – numerical FEE)*
SVF Software Verification Facility	To support the SW development, verify and validate on-board SW. The SVF allows to verify essential parts of the SW requirements (SW-SW integration tests & global tests) in an open and/or closed loop set-up, based on a simulated on-board time reference. *(ECSS-E-TM-10-21A class : Software Validation Facility - fully numerical)*
Dedicated system Simulators Instantiations (SAT-SIM, SIM-AIT)	Instantiations are derived from the SVF build status to perform system validation tests, and to prepare test or flight procedures (add-on and variation of model extensions towards SCOE or TM/TC interface (frame vs packet interfaces) *(ECSS-E-TM-10-21A class : Training Operations and Maintenance Simulator or Spacecraft AIV simulator pending use case)*

Test Bench Definitions / Objectives

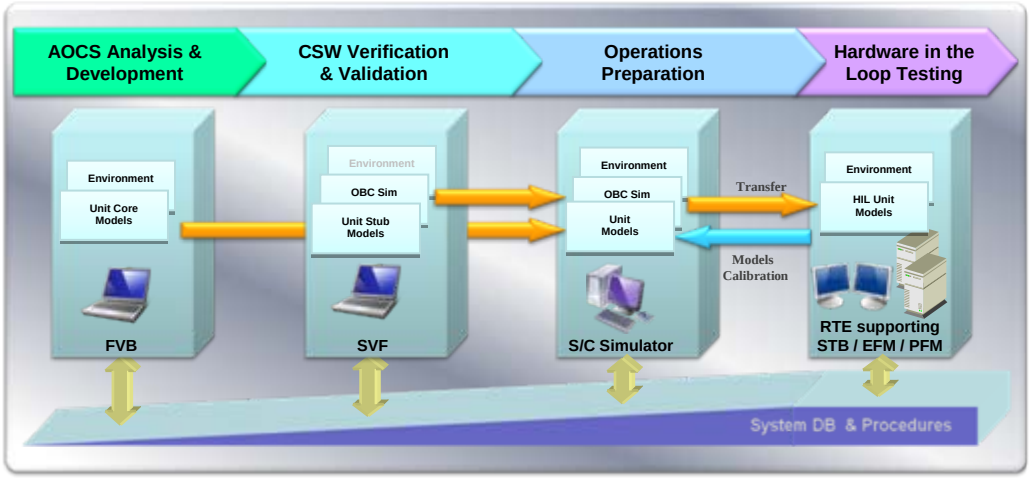
"Hybrid Benches"	
STB Software Test Bench	To support the development, verification and validation of the low level part of the SW (H/W-S/W interface) To calibrate the OBC numerical simulator against the real OBC, hence validating the SVF representativeness for functional verification.
EFM Electrical/Functional Model	To validate the functional chains and verify the HW/SW compatibility through open and closed loop tests To verify main mission requirements : proof of design To prepare the PFM verification and AIT campaign, including the (operational) validation of EGSE.
PFM/FM (Proto-) Flight Model	The flight configuration, in the end a 100% hardware configuration, but may also be supported at intermediate stages by simulated units of the real-time test environment, should the need arise. Proof of workmanship (acceptance) System validation activities In Orbit Testing…

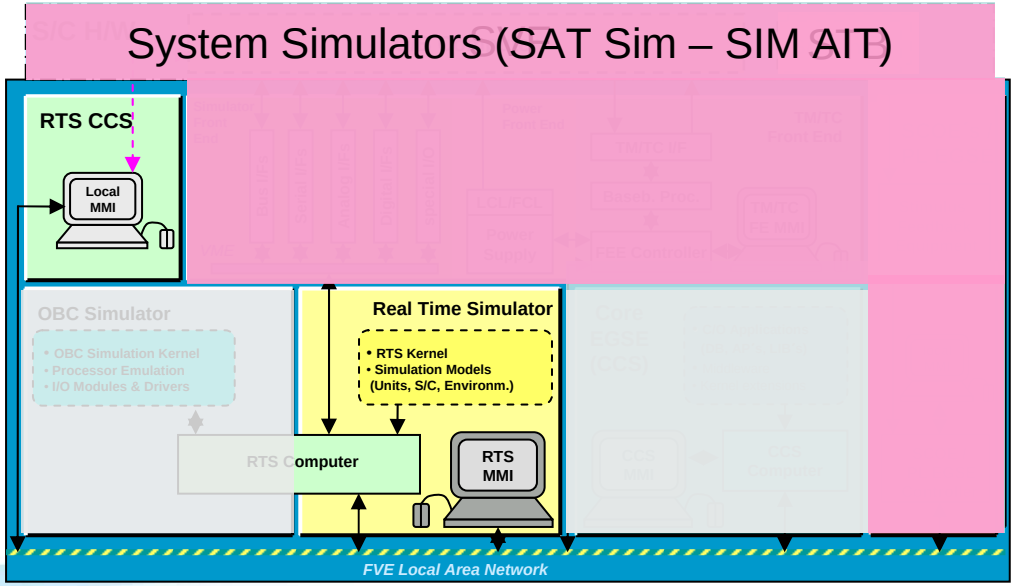
The Astrium Functional Verification Process



Underlying assumptions and difficulties

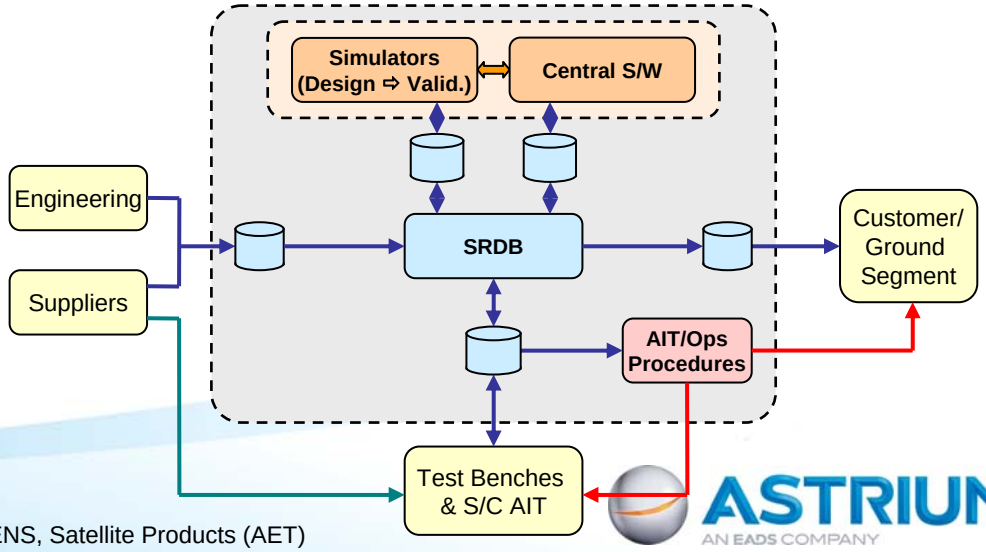
- Progressive infrastructure deployment
  - Model / SCOE continuity
  - Mastering of planning interdependencies
- Mastering benches multiple use cases
  - A single development lead
  - Avoidance of "CFI" to test teams
- The FVE bench tool kit : targeting the progressive build of the EFM
- Mastering HW-S/W integration at prime level
- Do the things once at the right place





Zoom on specificities

- Numerical OBC simulation
  - Models all subcomponents of the On Board Computer (OBC) including their redundancy
  - The processor itself is modelled via a processor emulator software library, allowing to load the image of the central software into the emulation and to process it – instruction by instruction.
  - Its representativeness wrt the OBC H/W-SW ICD and user manual and calibration wrt a physical model is key to allow a representative dynamic OBSW behaviour on numerical benches, thus formal V&V activities focussed on OBSW upper application layers
- Database
  - A central data management for the whole development process
  - A tool, but also a process



Support

Glossary

- **Validation** [ISO 9000:2000]
  - Confirmation, through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled
    - NOTE 1 The term “validated” is used to designate the corresponding status.
    - NOTE 2 The use conditions for validation can be real or simulated.
- **Verification** [ISO 9000:2000]
  - Confirmation through the provision of objective evidence that specified requirements have been fulfilled
    - NOTE 1 The term “verified” is used to designate the corresponding status.
    - NOTE 2 Confirmation can comprise activities such as
      - performing alternative calculations
      - comparing a new design specification with a similar proven design specification
      - undertaking tests and demonstrations, and reviewing documents prior to issue.