ALTARICA evaluation for Space activity

Written by M.TURIN GTI6 for ESA

Space projects problematic

Space projects

Long mission (spacecrafts), high availability (launchers)
Fault tolerance : no single point failure
Safety classification : catastrophic for some mission phases
Qualification under prime and ESA responsibility : no certification

Space technologies:

Radiation tolerance to SEU “single event upset”
Various mission specific software => reusability difficult
Redundancy management and FDIR => complex validation
Safety properties to be proven by evidence

Overall system engineering & software process
will have to be improved => Software crisis

ASSERT study objectives

ASSERT will enhance the classical engineering approach by a proof-based method encompassing the full system and software life-cycle supported by a well defined automated process.

ASSERT will apply this process on a standardized approach applicable to space activity by identifying system families

ASSERT will prove the validity of its new concepts by demonstration on real industrial cases, an intensive education and training program and diffusion of the results within a network of industrial partners (A.NET).

System Engineering Modelling and Verification methods

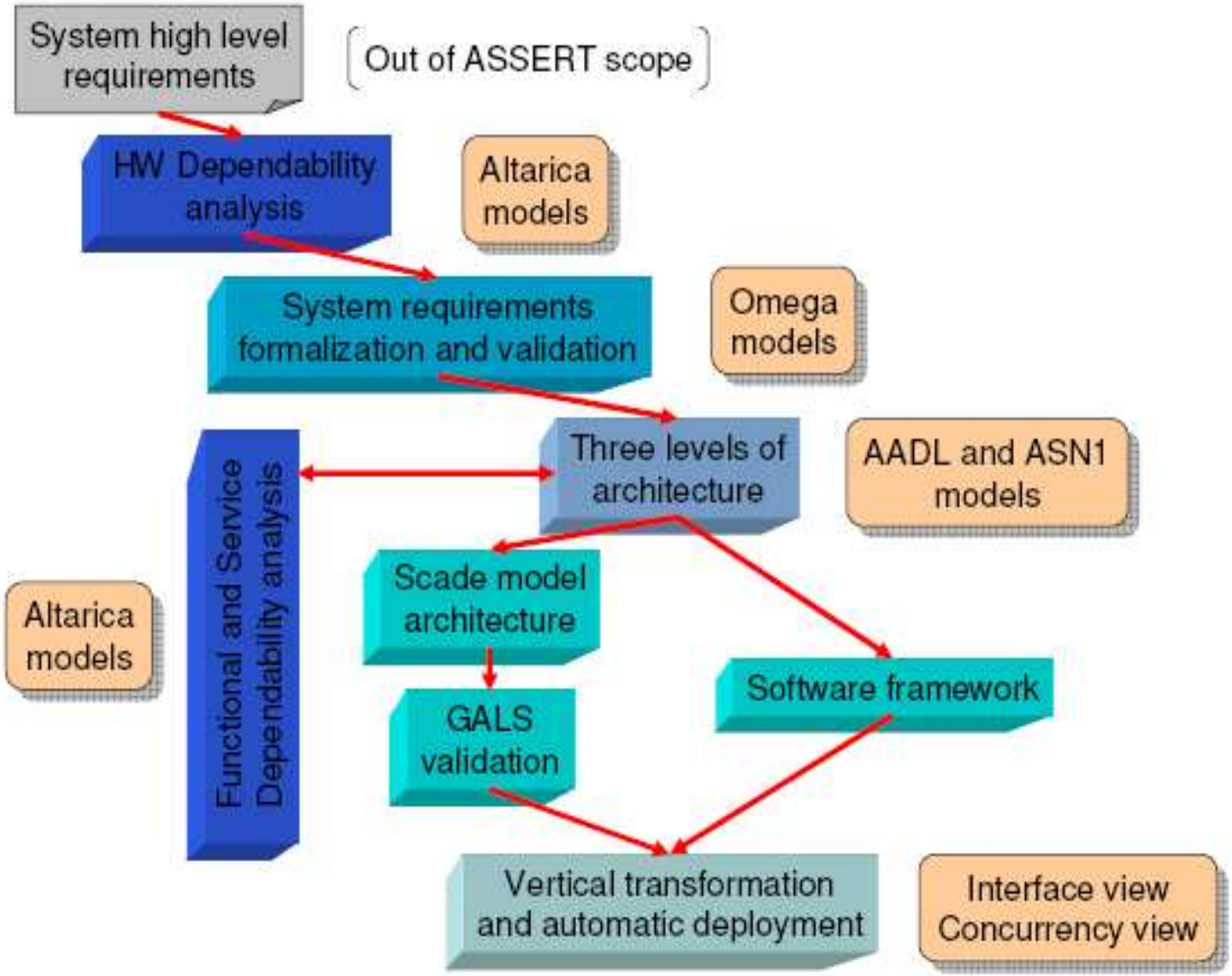
SEMV objectives

Independently of functional modelling and abstract architecture

SEMV will focus on
Safety & reliability requirements formalisation
Physical Architecture modelling
Verification of safety properties

Integrated tools to be defined for both functional and architectural views
AADL & UML have been selected for functional modelling
OCAS/ALTARICA for dysfunctional modelling
SCADE selected for synchronous architecture modelling
=> bridges shall be found to fulfil the automated process objective

One possible view of ASSERT process (MA3S)



ATV avionic architecture modelling

Done by ONERA with inputs from ASTRIUM
2 views : functional static & architectural
But many simplifications : dynamic behaviour not modelled

⇒ **Satisfactory results with limits :**

FMEA list : to be improved for an operational use

Failure tree : not usable for dynamic architecture with FDIR, not required by ESA

Sequence generation : very attractive (minimal cuts) but tool is slow

Reliability estimation : not evaluated but should be interesting (ARALIA…)

ALTARICA modelling remaining questions

FDIR modelling

SEU modelling : transient failure to be taken into account
Interaction with functional modelling : SCADE to ALTARICA translation ?
Dynamic architecture with failure propagation from hardware architecture & feedback to functional modes (FDIR, degraded modes)
Sequence generation, minimal cut, probability estimation
Model checking possibility ?

Failure propagation inside software models

Software partitioning according to SW category ?
Fault containment region, Middleware modelling

Reliability modelling

Stand-by redundancy & Active redundancy modelling
Fault tolerant architecture (TMR)
Failure detector performances (alarm rate, undetected error rate)
Reliability computation for several years mission
FMEA automatic documentation

ASSERT problematic

ALTARICA has not the objective to do functional analysis

Mapping with organic architecture is mandatory to analyse the failure effects

But maintaining several views : functional , organic and RAMS all along the project raises several problems :
- How the modelling will be maintained at a good level of detail
- How we can do models transformation accurately if the semantic are different

ALTARICA bridge with other tools

Translation from/to AADL : limitations ?

SMV model checker or any other prover ?

SCADE translation ?

Other tools (Dassault Aviation)