Using Aadl To Support Avionics Architecture Refinement And Selection

J. Delange[1], A. Jung[1], A.-E. Rugina[2], J.-F. Soucaille[2]
ESA[1] / Astrium Satellites[2]

In practice, the selection of an avionics architecture is performed by using a refinement process that starts with the identification of the necessary functions (both related to the platform and the payload) and of their interactions (in terms of data flows) from the mission requirements. Non-functional requirements are allocated to the functions (e.g., maximum processing necessary power, maximum mass) and data flows (e.g., data transmission rate). They represent constraints to be taken into account in the physical allocation of functions on devices and of data flows on on-board busses. The architect’s expertise and background (e.g. knowledge of legacy components) are complemented by a set of avionics-specific analyses in order to perform the tradeoffs and select the final architecture. In the traditional avionics architecture selection process, each type of analysis is based on a dedicated model, some of which (e.g., RAMS, FDIR, bus frame definition) require substantial amount of training to be used effectively. Using an architectural model to support the architecture refinement process has several advantages: (1) it traces the decisions through refinement links, (2) it represents a single input for the various analyses, guaranteeing overall consistency, (3) it favours reuse provided that the model can instantiate off-the-shelf functional and physical components.

AADL (Architecture Analysis and Design Language) is a candidate for supporting the above-mentioned architecture refinement and analysis approach. AADL has been standardized in 2004 under the auspices of the International Society of Automotive Engineers (SAE), to support the design and analysis of complex real-time safety-critical systems in avionics, automotive, space and other application domains. AADL provides a standardized textual and graphical notation for describing software and hardware system architectures. The serious consideration of AADL by the embedded safety-critical industry is justified by AADL’s advanced support for modeling reconfigurable architectures and for analyzing quality attributes, even if the available tool support (other than in-house tools) is quite scarce yet.

We present here a synthesis of the results of two studies: “ARAM” (performed by ESA) and “Guidelines for the selection of Architectures” (performed by Astrium Satellites for ESA). Both studies excersised the architecture selection process using the AADL language and AADL-related available tools in order to sketch AADL modelling guidelines and to identify existing or to-be-developed supporting tools.

The ARAM study aims at establishing a process for the design of avionics architecture based on three main steps. Starting from mission requirements definition (step 1), it provides a functional description of the system (step 2) and refines it to specify implementation concerns (step 3).The overall process is supported by the AADL from the high-level representation (step 1, with generic components such as system or abstract) to the implementation (step 3 with specific components) The use of a unique language provides the ability to check model compliance between each step. For that purpose, we use the Requirement Enforcement Analysis Language (REAL, available in the Ocarina AADL tool-chain) to validate one model with another. REAL is a language that analyzes models using a rigorous approach: theorems are bound to AADL components and later checked with a dedicated solver according to components characteristics (properties, sub-components, etc.). Such a method is currently used to check functional requirements against mission criteria and system implementation against functional description.

Currently, the ARAM process was exercised using existing space projects definition to define mission requirements, functional description and system implementation. Validation aspects were used to assess and check mass or power requirements. This study is however still in progress and will connect system specification with external validation tools to check other requirements (FDIR, RAMS, resources dimensioning, etc.).

In the study “Guidelines for the Selection of Architectures”, the architecture selection process was applied to the Solar Orbiter mission, developed by ESA in collaboration with NASA to carry an extensive set of scientific instruments to the near-Sun environment. In terms of AADL tools, the experiment relied on ADELE4.3.1 and OSATE2.0 for editing the AADL model (traceability to the textual requirements being captured using the Topcased-Req tool) and suggested the necessity of analysis tools related to:

- Power & mass analysis: comparison of the system power/mass to the sum of the functions/components requirements taking into account a specified margin for each of them.
- Reliability and availability analyses: based on annotations related to fault, recovery and propagation rates of functions or components.
- Resources analysis (memory and CPU load)
- Data latency: coarse (based on latency annotations on flow paths) and fine-grained (based on behavioural descriptions of components)
- Bus load: coarse (based and bandwidth budgets on flow paths and capacities) and fine-grained (to support for example the frame definition)
- Design consistency and correctness checks

To summarize, both studies resulted in:

- Feedback on the suitability of AADL for the intended architecture selection process: the language is suitable since it supports architecture refinement and annotations for analyses. We also identified possible improvements related to inheritance mechanisms and flow paths.
- Proposals of sets of AADL properties to support the suggested analyses. It would be relevant to converge on a set of properties to be added to the AADL standard property set. This would allow avoiding overlapping property sets and would facilitate implementation of tool support avoiding incompatibility of models potentially coming from different parties.
- Analysis tools' identification, preliminary specifications and even some proof-of-concept implementations in the context of "ARAM".

Feedback on the AADL-related available tools (bug reports and missing feature reports).