A Modelling and Analysis Framework for Avionics Systems

Visar Januzaj
Technische Universität Darmstadt,
Formal Methods in Systems Engineering
Darmstadt, Germany
Email: januzaj@forsyte.de

Ralf Mauersberger
EADS Innovation Works
Ottobrunn, Germany
Email: ralf.mauersberger@eads.net

Florian Biechele
EADS Defence & Security
Manching, Germany
Email: florian.biechele@eads.com

***Abstract*—The new paradigm of Integrated Modular Avionics (IMA) necessitates the analysis and validation of non-functional requirements for IMA systems. This includes the analysis of their performability. We present an initial approach of a performance modelling framework, based on the SAE standardised Architecture & Analysis Design Language (AADL). The proposed framework is a hybrid of static and dynamic systems analysis and includes aspects of performance evaluation.**

***Index Terms*—Avionics systems, modelling, analysis, system blueprints**

I. Introduction

Avionics systems have traditionally been implemented as federated systems with a dedicated processor for each function. While this has favourable effects on fault containment, its major drawbacks are high demand on spatial and power resources onboard the aircraft as well as high maintenance costs. To overcome these issues the *Integrated Modular Avionics* (IMA) [1] defines avionics systems as an integrated system with multiple functions hosted on a cabinet of processors. The binding between hardware and software components is defined in so called system configuration tables or *blueprints*. Despite its advantages, IMA demands sophisticated analysis of avionics systems. Thus a *blueprint generation* requires foregoing system analysis, e.g., schedulability analysis, to assure a correct operation of avionics software so that deadlines are met and memory resources are sufficient. To achieve a successful application of the IMA concept in the avionics domain, supporting techniques are essential for blueprints generation and their integration into the system development process.

We present a *performance modelling framework* consisting of a chain of actions, which enable the automatic generation of blueprints for IMA systems. Our framework not only proposes a method for execution time prediction in modern avionics systems, more importantly, it shows how those predictions can be integrated and used for the determination of stable and feasible system configurations (blueprints). In order to support the IMA technology we use the SAE standardised modelling and analysis language AADL [3], [4] which offers an abstract but precise description of the components of a system architecture and facilitates the application of performance analyses.

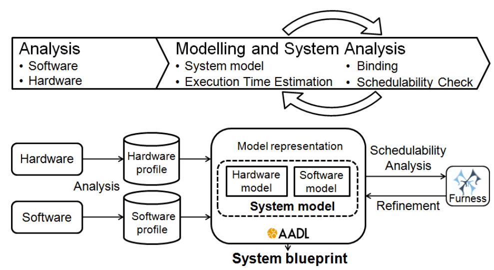

Fig. 1. Our Performance Modelling Framework.

II. The Performance Modelling Framework

Figure 1 shows the two stages of our modelling and analysis approach. Within the first stage, *component analysis*, we separately analyse the hardware and software components. This analysis concerns the execution time prediction and aims at generating corresponding *profiles* for each component. For the sake of simplicity the *hardware analysis* is carried out on a test-based manner yielding a hardware-parametrisable description of the measured execution time. The *software analysis* extracts the structure of the source code and calculates a symbolic execution time estimation. To achieve this we perform code instrumentation using the Compiler Infrastructure LLVM [6]. The computed profiles provide the necessary data for the estimation of the execution time of a software bound to a specific hardware and play a key role in the schedulability analysis process.

In the second stage, *modelling and system analysis*, we model in AADL the hardware and software components and compute a set of possible valid system configurations (bindings). For each computed binding between the hardware and software components we calculate the estimated execution time of the software components. Finally, we check if the modelled system is schedulable considering the current binding. We repeat this step until we find a feasible system configuration and subsequently generate the corresponding *blueprint*. The *schedulability analysis* checks the compliance of thread scheduling constraints using the Furness toolset [5]. Furness applies the ACSR [2] process algebra to determine schedulability. If a model is not schedulable Furness displays a failing trace (a timed system trace). Otherwise, it shows an analysis of best-case and worst-case time responses [5], thus facilitating the validation of various system configurations and the establishment of a thoroughly feasible system deployment.

REFERENCES

[1] Aeronautical Radio Inc. *Design Guide for Integrated Modular Avionics ARINC Report 651-1.* November 1997.

[2] Brémond-Grégoire, Patrice and Lee, Insup and Gerber, Richard. *ACSR: An algebra of communication shared resources with dense time and priorities.* In Proceedings of CONCUR'93. 417-431. 1993.

[3] Feiler, Peter H., Gluch, David P. and Hudak, John, J. *The Architecture Analysis & Design Language (AADL): An Introduction* (CMU/SEI-2006-TN-011). Pittsburgh.

[4] Society of Automotive Engineers. *SAE Standards: Architecture Analysis & Design Language (AADL)* AS5506 (November 2004) and AS5506/1 (June 2006).

[5] Furness website: http://www.furnesstoolset.com

[6] LLVM website: http://www.llvm.org