Chapter 9
Requirements Refinement and Component Reuse: The FoReVer Contract-Based Approach

Laura Baracchi
Intecs, Italy

Alessandro Cimatti
FBK-Irst, Italy

Gerald Garcia
Thales Alenia Space, France

Silvia Mazzini
Intecs, Italy

Stefano Puri
Intecs, Italy

Stefano Tonetta
FBK-Irst, Italy

ABSTRACT

The development of complex computer-based systems poses two fundamental challenges. On one side, the architectural decomposition must be complemented by a suitable refinement of the requirements. On the other side, it is fundamental to provide the means for component reuse in order to limit development costs. In this chapter, the authors discuss the approach taken in FoReVeR, a project funded by the European Space Agency (ESA), where these two issues are tackled in the setting of space systems. The approach taken in FoReVeR is based on the idea of contracts, which allow one to formally specify the requirements of components at different levels of abstraction and to formally prove the correctness of requirements decomposition. In particular, the authors show how system-level requirements can be progressively refined into software requirements and how the contract-based framework supports the reuse of the components of a reference architecture under development by ESA. The authors discuss how the proposed solution has been integrated in a space development process and present the results of case studies.

INTRODUCTION

The top-down design of complex critical system poses two fundamental challenges. The first one is the refinement of requirements, along with the progressive decomposition of the system architecture. In general, the quality and the traceability of requirements are fundamental for the whole design. Flaws in the requirements are in fact recognized as a major source of problems

DOI: 10.4018/978-1-4666-6194-3.ch009

Copyright © 2014, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

in the development, and may require major revisions in the advanced phases of the development cycle (Lutz, 1993). The second challenge is to enable for a correct reuse of (previously certified) components, which can lead to huge savings in development and certification costs. Unfortunately, the composition of correct components does not necessarily result in a correct system.

In this chapter we report how these issues have been addressed, in the context of space systems, within the FoReVeR project (see https://es.fbk.eu/projects/forever/). FoReVer (Functional Requirements and Verification Techniques for the Software Reference Architecture) is a European Space Agency (ESA) study conducted by a consortium led by Intecs with partners Thales Alenia Space France (TAS-F) and Fondazione Bruno Kessler (FBK).

The goal of the FoReVer project was to define an integrated methodology to introduce the formal verification of system properties from the early stages of the development process. The methodology had to be complemented by supporting toolset, to rely on a model-based approach, to allow the designers to check the correctness of model refinements, and to enable full traceability of design choices along the whole development process. Moreover, the study had to cover the refinement of the avionics system-level properties down to the software level, in order to enable the reuse of software components implemented in the On-Board Software Reference Architecture (OBSW-RA). The OBSW-RA is a reference architecture defined by the SAVOIR-FAIRE working group, as part of a large ESA initiative on Space AVionics Open Interface aRchitecture (SAVOIR), and was recently consolidated by several studies, the most recent of which is the ESA TRP COrDeT2 project (see http://cordet.gmv.com/).

The FoReVer methodology builds upon the Model-Based Space System Engineering process (MBSSE) derived in the System and Software Functional Requirement Techniques study (SSFRT) ESA study (Mazzini, Puri, Olive, Burte, Paccagnini, & Tronci, 2009). MBSSE is focused on the application of model-based engineering technologies based on SysML to support the space system and software development processes, from mission level requirements to software implementation through model refinements and translations.

FoReVer enriches the MBSSE process with the introduction of contract-based formal verification of properties, at different stages from system to software level, through a step-wise refinement of components. The contract-based approach allows to combine the top-down process of MBSSE with the reuse of OBSW-RA components, which represent a bottom-up driver in the process to ensure convergence to a solution compatible with the OBSW-RA.

In FoReVer, contract-based reasoning relies on the formalism proposed in (Cimatti & Tonetta, 2012), where contracts are specified in a language that is natural and expressive to formalize requirements of embedded systems (Cimatti, Roveri, Susi, & Tonetta, 2012). The underlying temporal-logic formulas (Cimatti, Roveri, & Tonetta, 2009) represent assertions on the possible interaction of each component with its environment. Tool support for contract reasoning (e.g. checking the correctness of refimenents) is based on OCRA (Cimatti, Dorigatti, & Tonetta, 2013), a tool for the verification of logic-based contract refinement for embedded systems, able to prove the correctness of contract refinements by reduction to a set of entailments in temporal logic. The reasoning engines used for verification of logic-based contracts refinement are provided by NuSMV3 (https://es.fbk.eu/tools/nusmv3/), an extended version of the NuSMV symbolic model checker.

In order to support a model-driven component-based methodology, the tools support in FoReVer is based on an enhanced version of CHESS (Mazzini, Puri, Veran, Vardanega, Panunzio, Santamaria, & Zovi, 2011). The CHESS component model is fully compatible with the Space Component Model adopted by the OBSW-RA. With FoReVer, CHESS

31 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/requirements-refinement-and-component-reuse/116111

Related Content

A Centralized Autonomous System of Cooperation for UAVs- Monitoring and USVs- Cleaning
Salima Bella, Assia Belbachirand Ghalem Belalem (2018). *International Journal of Software Innovation (pp. 50-76).*
www.irma-international.org/article/a-centralized-autonomous-system-of-cooperation-for-uavs--monitoring-and-usvs--cleaning/201485

A Survey on Secure Software Development Lifecycles
José Fonsecaand Marco Vieira (2014). *Software Design and Development: Concepts, Methodologies, Tools, and Applications (pp. 17-33).*
www.irma-international.org/chapter/survey-secure-software-development-lifecycles/77697

Decision Rule for Investment in Frameworks of Reuse
Roy Gelbard (2009). *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications (pp. 140-147).*
www.irma-international.org/chapter/decision-rule-investment-frameworks-reuse/21067

Implementation of Human-Machine Interface Module and Control System Based on Controller Area Network
H. Mohammed Ali, S. Radhika, G. Vanya Sreeand Ramya Maranan (2023). *Cyber-Physical Systems and Supporting Technologies for Industrial Automation (pp. 229-244).*
www.irma-international.org/chapter/implementation-of-human-machine-interface-module-and-control-system-based-on-controller-area-network/328503

The Library Big Data Research: Status and Directions
Shaochun Xu, Wencai Du, Chunning Wangand Dapeng Liu (2017). *International Journal of Software Innovation (pp. 77-88).*
www.irma-international.org/article/the-library-big-data-research-status-and-directions/182538