HAL open science

Adequacy of contract grammars for component certification

Alejandra Ruiz Huascar Espinoza, Tim Kelly

▶ To cite this version:

Alejandra Ruiz Huascar Espinoza, Tim Kelly. Adequacy of contract grammars for component certification. Safecomp 2013 FastAbstract, Sep 2013, Toulouse, France. pp.NC. hal-00926503

HAL Id: hal-00926503
https://hal.science/hal-00926503

Submitted on 9 Jan 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Adequacy of contract grammars for component certification

Alejandra Ruiz, Huascar Espinoza
ICT-European Software Institute Division
TECNALIA
Zamudio, Spain
{alejandra.ruiz, huascar.espinoza}@tecnalia.com

Tim Kelly
Department of Computer Science
University of York
York, United Kingdom
tim.kelly@cs.york.ac.uk

***Abstract*— The use of contracts in component-based development is a well-established approach. However there exists a wide range of views as to the nature of the contracts that are necessary to support safety-critical systems development, assurance and certification. Different standards and projects have tried to reduce ambiguity and propose the best practice in this area. In this paper we present work that moves one step further forward with the creation of a methodology and grammar that incorporates encompasses and helps structure current models of 'safety contracts'.**

Keywords*— *component; certification, contracts, grammar

I. Introduction

As systems become increasingly complex and distributed development becomes increasingly commonplace, there has been greater interest in component-based and contract-based approaches to system development and assurance. In parallel with this, certification standards are increasingly supporting the the notion of modular (component) certification. For example, DO-297 [1] addresses this topic in the context of modular avionics and the concept of SEooC (safety element out of context) has been introduced in the new automotive safety standard ISO 26262 [2]. These new concepts are not easy to apply. Ruiz et al [10] has previously described the difficulties faced by industry when attempting to apply the SEooC concept (particularly with respect to managing assumptions). Contract based approaches can help structure and manage the activities associated with compositional certification. .

II. Technical Approaches

A number of different technical approaches to contract specification have been studied. Each of them typically focuses on solving one objective. There are some identified reasons behind formalizing contracts such as [11]:

- Avoid human errors
- Support for validation or checking
- Interoperability between different suppliers
- Facilitate the integration of the components within the system

The following table shows some of the approaches already explored for improving the definition of contracts:

TABLE I. Different Contract Technical approaches

Approach	**Description**	***Ref***
Formal language	Specification of a formal meta-modeling language for design contracts. It provides information about components behaviour, variables and interfaces but not the implementation	[3]
	Specification of a formalization of safety cases. Safety argumentation can be logical deduction, probabilistic, expert judgement or historical experience. Formalizing some elements supports precision and cheching methods	[12]
Metamodel	The 'Rich Component' Metamodel focuses on the integration of component-based design by the use of contracts from different perspectives: such as operational actors, functions, logical components or technical components.	[6]
Reference architecture	In different domains there have been initiatives to define a reference architecture with an open API e.g. AUTOSAR. These reference architectures can be decomposed into different components. The integration of these components is implementation independent and is aided by well-defined interfaces	[7] [13]
Properties modelling	Formal and structured property modelling .	[8]
Pattern	Definition of a generic pattern for safety case contracts. They propose the GSN notation as a way to structure agreements between safety case modules.	[9]

All of these approaches try to solve parts the whole problem from different perspectives. Some approaches, such as those that concentrate on defining reference architectures, focus on design standardization and component integration rather than certification. (Although an argument can be made that they may reduce the costs of certification through establishing standardized interfaces.)

III. High Level guidance

Different assurance and certification standards have addressed the problem of component-based assurance in different ways. Here, we focus especially on the avionics and automotive domains. In the automotive domain, the introduction of the Safety Element of Context (SEooC) together with the standard ISO 26262 [2] has opened the door to modular approaches regarding functional safety. An example of a safety-oriented 'contract' can be seen in ISO 26262 [2], where the term Development Interface Agreement (DIA) is used to defines the procedures and responsibilities allocated within distributed developments for items and elements. In the DIA the supplier should exchange with the customer information such as: feedback about conflicts, completeness, consistency, etc.; technological limitations, behaviour models, incl. fault models, feedback about boundary between the component and its environment.

In the avionics domain we can find similar requirements with respect to module and application reuse within an IMA (Integrated Modular Avionics) platform. In DO-297 [1] (amongst other requirements) it is required that limitations, assumptions, etc. are documented and a usage domain analysis performance to ensure that any component is being reused in the a way that is compatible with the original design intent.

Other aerospace avionics guidelines such as AC 20-148 [4] concerning reusable software components indicate that in order to reuse components, stakeholders must identify any installation, safety, operational, functional and performance possible concerns. Developers need to state clearly the DO-178B objectives that are fully and partially addressed, and how compliance has been achieved. They need to state clearly the failure conditions, safety features, protection mechanism, architecture limitations, software levels, interface specification and the process for certification. AC 20-170 [5] defines incremental acceptance as, "A process for obtaining credit toward approval and certification by accepting or finding that an IMA module, and/or off-aircraft IMA system complies with specific requirements. This incremental acceptance is divided into tasks. Credit granted for individual tasks contributes to the overall certification goal." This definition implies that the process in which the system assurance is performed is also important. At every stage some form of recognition is submitted in relation which a compliance data package. The process is divided into 6 tasks: Module acceptance; Application acceptance; IMA system acceptance, Aircraft integration of IMA system, Change and reuse of modules or applications. Reuse can be done at Task 1and 2 level.

IV. COMPARISONS

Our on-going work addresses the challenge of integrating the existing approaches described in the previous sections. In doing this, we hope to improve consistency of approach across and reduce uncertainty as to the necessary considerations in safety-oriented contract specification and management.

Guidelines from the standards offer the best practices and interpretations of the standards in order to comply with certain requirements. Those best practices can be modelled within the different technical approaches and impact on the methodology for the system development. Different technical measures can be put into place in order to assure the correct and complete following of the guidance and practices.

In our approach we propose to formalized contracts through an well defined and structured contract 'grammar' to support how users may systematically assure safety of their system while integrating components. In order to do it we propose the definition of a BNF (Backus Normal Form or Backus–Naur Form) grammar. In this structure we will take into account the different views of contracts. AC 20-148 states that, "identify any installation, safety, operational, functional, or performance concern". We organise our contract grammar around these aspects to help identify such concerns. Fenn [9] proposes to use argumentation not only on safety cases but also on safety contracts, so our grammar should support argumentation. Rusby [13] has previous identified different types of argumentation. These types can be used to help provide extra structure to the argumentation aspects of the contract grammar.

One of the benefits of formalizing safety contracts will be the possibly of tool support for checking or generating contracts. We are using Xtext [14] as the technology to implement our grammar and be able to interoperate with other future tools. Moreover, with the provision of a defined grammar for safety contracts we will be able to support validation of contracts (e.g. helping identify incomplete contracts).

ACKNOWLEDGMENT

The research leading to these results has received funding from the FP7 programme under grant agreement n° 289011 (OPENCOSS) and nº608945 (Safe Adapt)

REFERENCES

[1] RTCA DO-297/EUROCAE ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

[2] International Organization for Standardization (ISO), ISO26262 Road vehicles – Functional safety, ISO, Nov 2011

[3] D.2.5.4 Contract Specification Language (CSL); SPEEDS Project; Deliverable; Rev. 1.0.1; April 2008: URL: http://speeds.eu.com/ downloads/D_2_5_4_RE_Contract_Specification_Language.pdf; PDF-Document; Last visit: 2013-02-13

[4] FAA Advisory Circular: AC 20 148 Reusable Software Components

[5] FAA Advisory Circulation AC 20-170

[6] D_SP1_R3.3_a_M3 Meta-Model Concepts for RTP V; CESAR Project; Deliverable. http://www.cesarproject.eu/index.php?id=47&L=0; PDF-Document; Last visit; 2013-02-12

[7] Fürst S.: AUTOSAR – An open standardized software architecture for the automotive industry. 1st AUTOSAR open conference & 8th AUTOSAR premium member conference, Detroit, US, Oct. 2005

[8] ATTEST2 Project, URL: http://www.atesst.org Last visit: 25/06/2013

[9] J. Fenn, R. Hawkins, P. Williams, and T. Kelly, "Safety Case Composition Using Contracts -Refinements based on Feedback from an Industrial Case Study," in Proceedings of 15th Safety Critical Systems Symposium(SSS'07), February 2007

[10] A. Ruiz, H. Espinoza, F. Tagliablò, S. Torchiaro, A. Melzi, "A Preliminary Study towards a Quantitative Approach for Compositional Safety Assurance" Proceedings of 21st Safety Critical Systems Symposium, February 2013

[11] Machine-checkable Assurance Case Language http://www.omg.org/cgi-bin/doc?sysa/2012-9-4

[12] J. Rushby, "Formalism in safety cases," in Making Systems Safer: Proceedings of the Eighteenth Safety-Critical Systems Symposium, Springer, 2010, pp. 3–17.

[13] ARINC 653 Avionics Application Software Standard Interface

[14] Xtext, » http://www.eclipse.org/Xtext