Towards a multi-view point safety contract

Alejandra Ruiz, Tim Kelly, Huascar Espinoza

Towards a multi-view point safety contract

Alejandra Ruiz[1], Tim Kelly[2], Huascar Espinoza[1]

[1] ICT-European Software Institute, TECNALIA, Parque Tecnológico Ed. 202, Zamudio, Spain
{alejandra.ruiz, huascar.espinoza}@tecnalia.com
[2] Department of Computer Science, University of York, York, United Kingdom
tim.kelly@cs.york.ac.uk

Abstract. Use of contracts in component based development is a well-known approach in the development of complex systems. However there are challenges when using this approach when dealing with safety, and safety assurance, properties. Safety is a system property and because of that, it can be hard to define the contribution of components that have an impact on safety. Contract based approaches addressing safety have been proposed in the past regarding modular safety case development. In this paper we suggest a "multi viewpoint" contract approach where these many aspects are organized to address different stakeholder concerns.

Keywords. safety contract, certification, safety case, composition

1 Introduction

As systems become more and more complex and distributed development becomes common on many sectors, so do component-based and contract-based approaches. Safety critical systems are not different and modularity has been introduced on this area as well. However safety is a difficult property to decompose as it is system property.

In this paper we suggest a multi-viewpoint approach for the contract interfaces that makes contracts a more manageable instrument that support different stakeholders establish the validity of the contracts.

In section 2 we present the differences and similarities between design contracts, safety contracts and assurance contract approaches, in section 3 different contract based approaches are explained, in section 4 we draw out some of the key commonalities and variability in existing approaches. In section 5 we suggest the multi view approach for contracts. Finally in section 6 conclusions are described.

2 Design contract vs. safety contracts vs. assurance contracts

Component based approaches are seen as a common and well know strategy while dealing with complex systems. As systems have grown in complexity, so does the trend in using component-based development approaches.

However contract-based approaches differ when we see them from the development perspective and from the safety perspective. We can define design contracts as

those agreements made for development purposes where interfaces between components are identified and agreed in order to interoperate. The component is assumed to have a correctly functionality just by assuring the interfaces with others. From the safety perspective, safety is a whole system property and assuring the correct function of components does not mean that the (composed, integrated) system will remain safe.

As Espinoza remarks[3], "the challenge in such systems is to assess not only the certifiability of each component or module, but also its certifiability once it is in an 'integrated' state".

We have identified three steps in the use of contracts to support the certification of components. The first step is the use of **design contracts** to support the technical integration of different components within a system. Design contracts focus on the necessary conditions for correct component operation. In an integrated component configuration if component contracts are satisfied the set of components can be assumed to function correctly together.

The context in which the component is going to be integrated is important and as Ruiz [7] indicated for the SEooC (Safety Element out of Context) perspective the assumptions of the item can be understand as the context characterization. In addition, to support safety assessment, failure behaviors of components, and their behavior in the presence of failures, must be defined. Ruiz shows some needs of the industry in relation with the application of the SEooC concept and proposed the use of **safety contracts** as a possible strategy. A primary challenge is identifying all of the assumptions made and secondly envisaging all of the different contexts in which the element might be used.

The last step mentioned is that of **assurance contracts**. Assurance contracts define the set of claims that need to be made concerning a component to support its certification against a particular safety assurance standard. Different standards address this problem in different ways. In ISO 26262 [2] Development Interface Agreements (DIA) are described as a way to specify both procedures and responsibilities allocated to distributed developments for items and elements. The DIA includes information beyond technical safety by addressing procedural and confidence related issues. The use of DIAs is intended to help address risks such as: a supplier with inadequate capability, improper understanding or definition of the boundary of component and its interactions with its environment, or failing to fulfill requirements.

In the avionics domain we can find similar requirements while talking about modules and application reuse on an IMA (Integrated Modular Avionics) platform. In DO-297 [1] for reuse of component acceptance it is required that component limitations, assumptions, etc. are documented and a usage domain analysis is performed to ensure that it is being reused in the same way as it was originally intended. As in the automotive domain, in the avionics domain the adequacy of suppliers is a concern. Big companies such as Airbus are starting to put into practice a methodology to ensure the quality and capability of their suppliers specially for the critical functions. Yani presented [11] the plans for Airbus on the idea of extended airworthiness. The main issues being addressed were: delegation of authority, the cascade on certification requirement and the surveillance of suppliers

3 Existing Contract Approaches

The SPEEDS [4] project developed and implemented a formal meta-modeling language and the syntax of component contracts. These contracts define the premises and promises of the component in order to behave in a specific way and an attribute designating its viewpoint. Viewpoints have no formal semantics in SPEEDS but are used as a means of organizing contracts across a complete system specification. The specification of the *assumption* and *promise* assertions is the core of the contract; it presents the required capability of the component (associated with the viewpoint) [5].

CESAR [6] defined the CESAR Meta Model (CMM) that includes the concept of 'rich' components, which can be connected and integrated in hierarchies. There can be different kinds of rich components such as operational actors, functions, logical components or technical components depending on the perspective. CMM is based on an integration of component-based design with contracts based on input from SPEEDS project, EAST-ADL2 (traceability, verification and validation) from ATESST project and the own CESAR Requirements Management Meta-Model (RMM).

CHESS project [13] also defined a component model but focusing on safety, reliability, performance and robustness characteristics. This project proposed two different categories of views, the System Level and the Platform Independent Model (PIM). The set of views that conform each category was needed and as a whole described the component.

In the certification domain, also the concept of modular certification has been under study, e.g. by the UK IAWG (Industrial Avionics Working Group). Modular and incremental certification is seen as a strategy to deal with the cost of re-certification of change in relation with size and complexity of the system.

Both Kelly [9] and IAWG [8] have proposed approaches to represent contracts that record agreement in the composition of safety case modules. IAWG [8] proposed that the GSN is used in order to capture the rationale behind the safety contracts relationship. This way strategies, justifications, and context are also included on the contract and the rationale is made explicit.

4 Commonalities and Variabilities in Existing Approaches

Although there are differences between each type of contract as it has been shown on the previous section, there are also commonalities. Most of the different types of contracts presented beforerecord agreements in terms of *promises* and *premises*. It is the information behind those promises and premises what makes the contracts different.

Assurance contracts and safety contracts both need to deal with information which contributes to an adequate demonstration of system safety. Contracts identify the different characteristics or which specifies behavior for the components related where premises are valid and the promises or guarantee are ensured to be true.

The documentation of assumptions and intended context of use is also a common feature. They indicate the boundaries and operation conditions that ensure the correct and safe used of the component.

Premises and promises are the core of the contracts. Premises need to be validated before the contract promises can be fulfilled. Those premises are typically identified at the component level. Promises can be made at component level but also new promises can appear as the integration of components enables new promises (regarding the composition of components) to be made..

Promises and premises are closely interconnected. Guarantees identified at component level but those promises that are not ensured and validated by contracts could make the contracts not valid. It is also important to consider behaviors, not only nominal behavior but also failure and degraded behaviors are important to consider for both the safety contracts and assurance contracts.

5 A multi-viewpoint approach?

Multi-view point approaches to description and definition exist in a number of existing applications. The standard IEEE 1471 [12] suggests the use of views to rationalize and organize architectural descriptions. The views help document a particular perspective of a system that is of interest for a particular stakeholder.

Flood and Habli [10] have also proposed multi-view safety cases in order to facilitate the understanding of the safety argumentation abstracting those elements that are of interest or particular stakeholders.

We propose that safety contracts could also benefit from a multi-viewpoint approach. The types of contracts mentioned in previous sections can be regarded as offering different (but interrelated) viewpoints on a common problem.

Table 1. Examples for contract viewpoints

Viewpoint	Premise and promise nature	Concerns
Design contract	Component A, B and C are integrated in an IMA platform.	Communications and functionality
Safety contract	Ensure component isolation and interdependency	Failures, misbehaviors.
Assurance contract	Interpretation of the standard and how to comply with its objectives	Compliance with the standard's requirements

But all of these viewpoint are not complete isolated, premises and promises are inter-related. Even more, they linked to evidences and claims that argument safety of the system as a whole.

Using viewpoint will let us handle the different aspects in a unify framework, this way different type of contracts in a common and systematic way structuring the information and this way helping to assure completeness.

Managing contracts may be complex but with the suggested approach, we will give a process for component composition a structure, making it more manageable and linking safety behavior with safety properties.

6 Conclusions

There are a number of existing contract based approaches that can be said to contribute to safety assurance: design, safety and assurance contracts. Each addressing different but interrelated concerns. There are <common features>, and <differences> as we have suggested on section 4.

We suggest that like other domains, it would be useful to adopt a multi-viewpoint approach,. We have briefly illustrate what this might mean in a concept example. Further research is required to develop and evaluate this concept.

On the suggested approach there is a possible strategy for dealing with complexity with contracts however one important challenge for contracts haven't been analysis, that is managing different context. In a way this contexts are seen as assumptions in our proposal but how they can be declared in a way that facilitate the integration of these contexts haven't been studied.

Acknowledgment: The research leading to these results has received funding from the FP7 programme under grant agreement n° 289011 (OPENCOSS)

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. H. Espinoza, A. Ruiz, M. Sabetzadeh, and P. Panaroni, "Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems," wosocer, pp.1-6, 2011 First International Workshop on Software Certification, 2011
4. D.2.1.5 SPEEDS L-1 Meta-Model; SPEEDS Project; Deliverable; Rev. 1.0.1; May 2009: URL: http://speeds.eu.com/downloads/SPEEDS_Meta-Model.pdf; PDF-Document; Last visit: 2013-02-13
5. 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
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. 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
8. J. L. Fenn, R. D. Hawkins, P. J. Williams, T. P. Kelly, M. G. Banner, and Y. Oakshott, "The who, where, how, why and when of modular and incremental certification," in System Safety, 2007 2nd Institution of Engineering and Technology International Conference on, 2007, pp. 135–140.
9. T.P.Kelly. "Concepts and Principles of Compositional Safety Cases", (COMSA/2001/1/1) – Research Report commissioned by QuinetiQ

10. M. Flood and I. Habli, “Multi-view safety cases,” in 2011 6th IET International Conference on System Safety, 2011, pp. 1 –6.IEEE P1471 Recommended Practice for Architectural Description
13. D2.1 – CHESS Modelling Language and Editor CHESS Project; Deliverable. http://api.ning.com/files/iVO0Zl2n8N6um45WOOQNxCmXcgyO0JObBb7Vh2l4I0nJRW1AW6v5L5zTVxrz*x2t94IvKdDS8hEtQx9Lhh*etowoQWgaqzVC/D2.1CHESSModellingLanguageandeditor.pdf;PDF-Document; Last visit; 2013-06-18