A Contract and Facet Based Method for Modeling and Verification of Heterogeneous Systems Group: HIFI

A. Abdelkader Khouass[1,2] and J. Christian Attiogbé[1]
[1] Nantes Université, LS2N, UMR 6004, Nantes, France
[2] University of Tlemcen, LRIT, Algeria
abdelkader.khouass@univ-nantes.fr, christian.attiogbe@univ-nantes.fr

1 Introduction

Nowadays, the great scale of the needs in several sectors like air traffic control, railway, autonomous vehicles, etc, forces one to build complex systems. These systems are often built by assembling a huge number of hardware/software components. Their requirements force developers to use a wide variety of heterogeneous components. Consequently, the efficient modeling, composition and formal analysis of these heterogeneous systems is still challenging.

We aim at studying and alleviating the difficulties of practical modeling and integration of heterogeneous components.

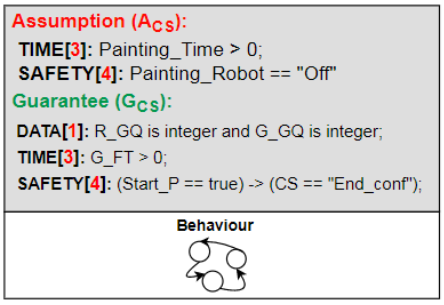
We build on contract-based approaches [1, 2]. Then, in [3] we introduced the notions of *facet*, *generalized contract*, *normalized component* and we proposed a method (named "ModelINg And veRifying heterogeneous sysTems with contractS" (Minarets)). A *facet* is a marker of the category of a property. As the properties of a complex system can be very general and heterogeneous, we use such facets to distinguish the sub-properties.

A *generalized contract* is an assume-guarantee contract extended by the integration of the various facets it may cover. A *normalized component* is a component equipped with a generalized contract, making it interoperable with other components which are normalized in the same way (see Figure 1). In the following, we give a brief description of our method.

2 An Overview of the Minarets Method

The method that we propose (Minarets) consists in, given a set of appropriately selected or predefined elementary components: i) normalizing these input components prior to their composition, ii) building a global heterogeneous system by composing the normalized components, and finally iii) analysing this global system with respect to the required properties. For this purpose, our method handles the following issues: ***i)*** Since elementary components are from various languages and cover different facets, a pragmatic means of composition is required: each component will be manipulated through its *generalized contract* written in an appropriate language. We consider PSL [3] as a wide purpose expressive language to describe generalized contracts.

Fig. 1: Normalized component: Control Station of a painting workshop [3]



ii) Global properties are heterogeneous; they should be clearly expressed, integrated and analysed. They will be expressed with a wide purpose language such as PSL; we will decompose them according to the identified agreed-upon facets and spread them along the analysis of composed components.

iii) Composition of elementary components should preserve their local contracts and should also

[3] Property Specification Language (PSL) https://ieeexplore.ieee.org/document/5446004

fit with the global-level properties. For instance, some facets required by an elementary component could be unnecessary for a given global assembly, or some facets required at a global assembly are missing at a component level. Therefore, we will weaken or strengthen the properties at the component level.
iv) Behaviours of components should be composable. For a given system we will assume *agreed-upon facets* such as data, functionality, time, safety, etc. This simplifies the composition of heterogeneous systems.
v) Global properties require heterogeneous formal analysis tools; this generates complexity. We choose to separate the concerns, so as to target various tools and try to ensure the global consistency.

The Minarets method integrates these solutions. We adopt a correct-by-construction approach for the assembly of components. Therefore, local compositions should preserve required properties of components by considering their contracts. In the same way, global properties may impact the components composition; therefore, global properties are decomposed and propagated through the used components when necessary. For the sake of brevity, we refer to our reports [3,4] for the detailed explanation of our Minarets method and for the experimentations of the car painting workshop, and the landing gear system (a known modeling benchmark).

Unlike [1] in our work we deal with heterogeneous components, we aim at reusing as much as possible existing components. Then, for the sake of mastering heterogeneity of component descriptions, we separate the behavioural part from the contract; this facilitates the composition of (A,G) contracts of the heterogeneous components and also the reuse of single behavioural components. In addition, the Ptolemy project [5] proposes an approach of interaction between heterogeneous components based on models of computation (MOC); here the heterogeneity is linked to different models of computation. From our point of view, this composition method is heavy, too general and constrains the use of contracts,

3 Conclusion

We have proposed the Minarets method for the modeling and the analysis of complex and heterogeneous systems. It is based on an extension of the traditional contracts, resulting in generalized contracts proposed as standard interfaces between various components. Generalized contracts are structured with several facets, depending on the concerns or the properties that we are dealing with. Our approach whith the generalized contracts empowers the idea of normalization of interfaces of components for easing the reused and composition of heterogeneous components.

Our future works will address the study of various policies for the decomposition of contracts; we will study more deeply the interferences between facets. Finally, we will propose tools to guide the users in normalizing, composing and verifying the heterogeneous components.

References

1. Benveniste, A., Caillaud, B., Nickovic, D., Passerone, R., Raclet, J., Reinkemeier, P., Sangiovanni-Vincentelli, A.L., Damm, W., Henzinger, T.A., Larsen, K.G.: Contracts for system design. Found. Trends Electron. Des. Autom. **12**(2-3), 124–400 (2018), https://doi.org/10.1561/1000000053
2. Chen, T., Chilton, C., Jonsson, B., Kwiatkowska, M.Z.: A compositional specification theory for component behaviours. In: Seidl, H. (ed.) Programming Languages and Systems - ESOP 2012, Held as ETAPS 2012, Estonia, Proceedings. LNCS, vol. 7211, pp. 148–168. Springer (2012), https://doi.org/10.1007/978-3-642-28869-2_8
3. Khouass, A.A., Attiogbé, J.C., Messabihi, M.: Multi-facets contract for modeling and verifying heterogeneous systems. In: Model and Data Engineering MEDI 2021, Estonia, 2021, Proceedings. LNCS, vol. 12732, pp. 41–49. Springer (2021), https://doi.org/10.1007/978-3-030-78428-7_4
4. Khouass, A., Attiogbé, C., Messabihi, M.: Modeling and analysis of the landing gear system with the generalized contracts. CoRR **abs/2111.10426** (2021), https://arxiv.org/abs/2111.10426
5. Lee, E.A.: Disciplined heterogeneous modeling - invited paper. In: Model Driven Engineering Languages and Systems - 13th International Conference, MODELS 2010, Proceedings, Part II. LNCS, vol. 6395, pp. 273–287. Springer (2010), https://doi.org/10.1007/978-3-642-16129-2_20