

Correct by Prognosis: Methodology for a Contract-based refinement of Evolution Models

Christoph Etzien ¹and Tayfun Gezgin ²

Abstract The scope of this paper is collaborative, distributed safety-critical systems building up a larger scale system of systems (SoS). Systems are independently designed and can operate autonomously following both global SoS- and individual goals. A major aspect of SoSs is the evolution over time, i.e. the change of its architecture as a result of changes in the context of the SoS or the changes of individual or global goals. We define a modeling concept for evolution specifying all possible changes of the SoS over time. This evolution model is used to generate and analyze future architectures enabling the prediction of future violations of static specifications. The challenge is to address the consistency of the evolution model with respect to the static specification of the SoS. This is achieved by deriving so called dynamicity contracts and thus restricting the evolution model in such a manner, that only correct architectures are produced.

¹ OFFIS – Institute for Information Technology, Escherweg 2,26121 Oldenburg, Germany - etzien@offis.de

² OFFIS – Institute for Information Technology, Escherweg 2,26121 Oldenburg, Germany - gezgin@offis.de