In Bulletin of the EATCS 68, 245–247. June 1999.

Author: Carlos Henrique Cabral Duarte (carlos.duarte@computer.org)

Title: *Proof-Theoretic Foundations for the Design of Extensible Software Systems*

Language of presentation: English

Promotor: Prof. Dr. Thomas S. E. Maibaum

Date of defence: 8th of February, 1999

Institution: Department of Computing
Imperial College of Science, Technology and Medicine
University of London

Abstract:

Extensible software systems have been increasingly demanded as a means of supporting in a more faithful way constantly changing user requirements and also as a necessary logical counterpart to rapidly evolving networking architectures. Such terms as open, reconfigurable, mobile and reflexive have been used to attempt to describe relevant facets of this kind of reactive system with dynamically varying functionality or structure. In this thesis, we not only characterise extensible systems but also study their rigorous design.

We advocate a proof-theoretic step-by-step approach to the development of extensible systems as a means of ensuring correctness, modularity and incrementability. By spelling out their characteristics and identifying corresponding logical constructions, we present as an original foundational contribution a first-order branching time logical system that seems to be appropriate as a basis for specification and verification. Even though our software process approach is proof-theoretic, we provide both model and proof theories for the proposed system, studying in the context of general logics important properties such as soundness, completeness and expressiveness. We argue that other logical systems proposed in the literature are not adequate to achieve the same desirable effects in design.

We also study particular software development approaches based on the actor model, on dynamic sub-classing and on meta-level architectures which could best underpin the rigorous design of extensible systems. Specific design principles are proposed in the form of derived inference rules with their application guidelines and composability notions are studied in terms of categories of theory presentations. We show that reasoning about their local properties can be carried out based only on such constructions but global properties may not be verified without the additional aid of a rely-guarantee discipline. A series of helpful theorems and realistic examples are developed to support and illustrate how our ideas can be effectively applied in practice.

Table of contents:

Author address: Banco Nacional de Desenvolvimento Econômico e Social
Av. Chile 100, Centro
Rio de Janeiro, RJ
20001-970 Brasil