Designing dependable process-oriented software

a CSP-based approach

Ph.D. thesis of Dusko Jovanovic

ISBN: 90-365-2334-6

Summary

This thesis advocates dependability as a crucial aspect of software quality. Process orientation, as it is defined in this thesis, concentrates on the notion of a process as a basic building component of a dataflow-centred software architecture. The dependability approach in the proposed variant of process orientation builds on a few specific strengths of the particular dataflow-centred architecture which is based on the principles of the CSP process algebra.

The CSP/CT process-oriented modelling and programming environment for control applications has been enriched in this work with various complementary instruments for raising dependability of concurrent software. In addition to the design methodology enhancement, the main deliverable is a graphical CASE tool, named gCSP, which facilitates modelling, visualizing and managing software models of evergrowing complexity. By manipulations of once developed models, the gCSP tool exploits the formal underpinning of the methodology to allow formal verification of the designs by automatically generating formal specification in the CSPm language. Efficient production and trusting the final outcome of the design—implementation code—is substantially increased by automatic code generation of C++ code compliant with the CTC++ implementation library for concurrent programming. In this thesis it is illustrated, worked out and shown on examples and mechatronic set-ups that the process-oriented CSP/CT framework is suitable for hosting various established dependability instruments: concurrent exception handling, N-version programming, logging, monitoring and several variants of watchdogs.

This thesis advocates: tool-based visual programming, investments of increasing computer capabilities in bearing overheads of dependability of complex software systems, separation of versatile software concerns at the modelling stage, and making software development an engineering discipline by predictability established on a mathematically-based development. This together is proposed for raising quality of (embedded) software in design time.