Safe Object-Oriented Software Cliffs Notes

February 20, 2006

Design By Contract

A program statement S exists to achieve some desired postcondition R after its execution. The statement S will only accomplish the state R if some precondition P is satisfied before S is executed.

$$\{P\}\, S\, \{R\}$$

Verified Design By Contract

All contracts are formally verified without making assumptions that cannot be justified or sacrificing soundness in other ways. The Escher project is a toolset to support Verified DBC with close to 100% automated verification.

- Code should serve only to implement a corresponding specification.
- The notation should support specifications based on abstract data models with refinement to implementation models.
- The notation should be designed to facilitate automated verification, avoiding the problems of notations based on programming languages.

Verification conditions are generated to express 47 separate aspects of correctness, including the following:

- Every method precondition is satisfied at each point of call.
- Every constructor and procedure satisfies its postcondition and postassertions.
- Every function delivers its declared result value.
- When one method overrides another and declares a new contract, the new contract respects the old.
- Class invariants are established by all constructors and preserved by all methods.
- Loop invariants are established and preserved.
- Loops terminate after a finite number of iterations.
- Assertions embedded within an implementation are satisfied.
- Behavioural properties specified by the user are satisfied.
- Explicit type conversions always succeed.