SE33010 Assignment Two - Alexander D Brown (adb9)

Moving from the Spiral Model to Formal Methods

The Spiral model of software development is a lifecycle which is intended for large, expensive and complicated projects, explicitly including risk management as part of the development process. Figure 1 depicts the overall process of the spiral model.

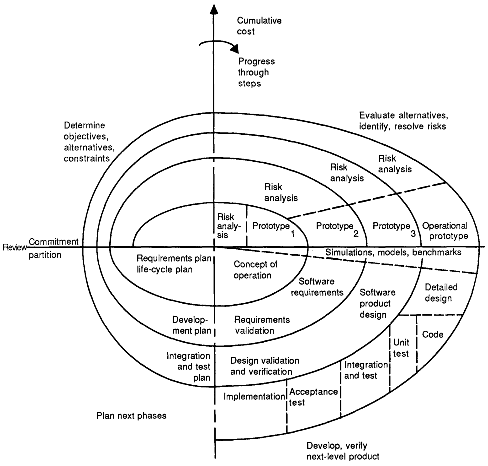

Figure 1: Spiral model of the software process[1]

Formal Methods of software development have many different flavours but focus upon proving the correctness of the produced software, typically through application of mathematical specification. Formal Methods are very useful for safety- or mission- critical systems; where traditional methods would have to rely on large amounts of testing.

Both methods start similarly; gathering requirements for the system. However the Spiral model focuses on both requirements and risk analysis whereas Formal Methods these requirements are used to build an abstract specification.

This report will focus on the Vienna Development Model (VDM) as the model for a Formal Development Method, however that are many others with different syntax or structures.

With VDM the two main focuses are on *Data Reification*: the development of abstract data types into concrete ones and *Operation Decomposition*: the development of algorithms from the implicit specification of functions and operations.

The first change that would need to be made is to build this abstract specification based on the requirements, defining the data types and operations which are needed to complete the system.

From this the first reification step is taken; each of these steps involve:

1. From the abstract data type specification ABS find a new representation REP
2. Find a *retrieve function* that relates ABS to REP
3. Prove that REP is *adequate* to represent ABS
4. Re-write functions and operations in terms of REP.
5. Prove that these new functions and operations preserve any data-type invariants of REP.
6. Prove that these new functions and operations model those of the original specification:
    - Prove that preconditions for operation OPA on ABS returns the same results on REP
    - Prove that the postconditions for operations OPA on ABS return the same results on REP given that the preconditions were met

References

[1] B.W. Boehm. A spiral model of software development and enhancement. *Computer*, 21(5):61–72, 1988.