Classical B and Atelier B

Marielle Petit-Doche

Systerel

April 15th, 2013

Historical

- *The B Book, Assigning Programs to Meanings* [Abrial1996]
- More than 20 years of practice in industry
- First important system : METEOR in 1998
- Used by main manufacturers : ALSTOM, SIEMENS, AREVA,...
- Lots of application in urban railway domain : CBTC, ZC, CC, PMI,..
- Some applications in mainline domain : KVB, Eurobalise,...
- Well adapted to develop critical software according to EN50128
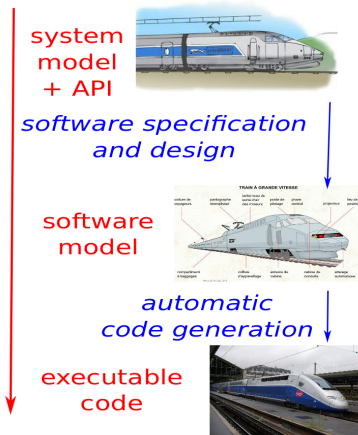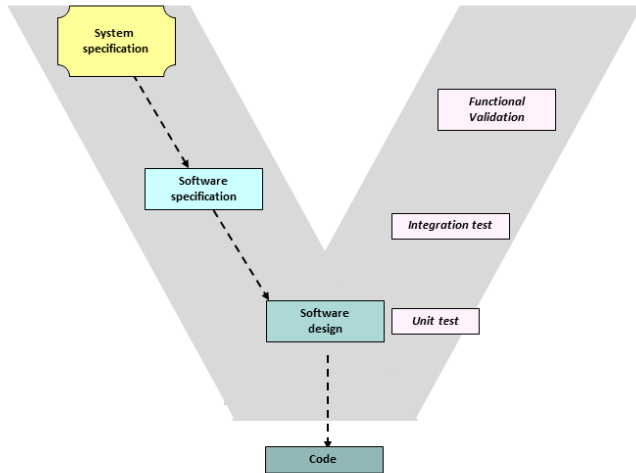
Main usage in railway industry

Classical B
Software Design :

- ▶ full functional description
- ▶ some safety constraints
- ▶ structured model
- ▶ refinement
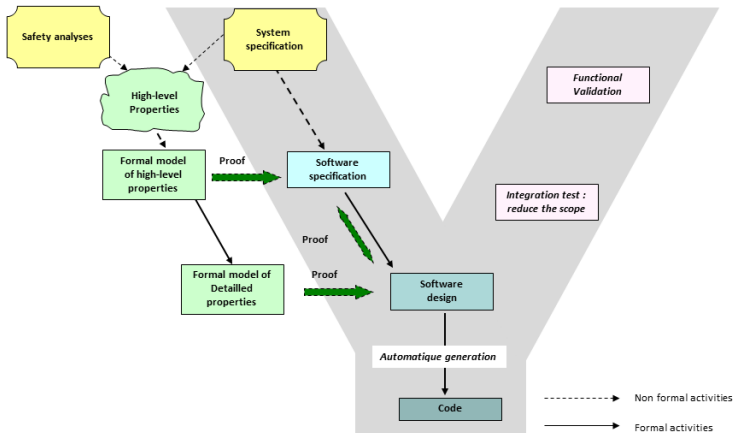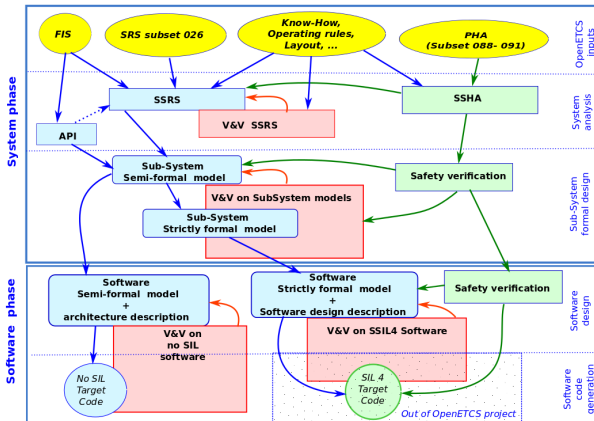- ▶ deterministic model to generate code

system
model
+ API

*software specification
and design*

software
model

*automatic
code generation*

executable
code

Classical B approach

- ▶ Language : first order logic + group theory (inherited from language Z, Hoare predicates,...)
- ▶ Structured models : Components to describe the software architecture
- ▶ Operations, Invariants
- ▶ Correct by construction approach
- ▶ Formal proof (partially interactive)
- ▶ Automatic code translation (C, Ada,...)
- ▶ Industrial tool : Atelier B (now free but close source)

From V-cycle...
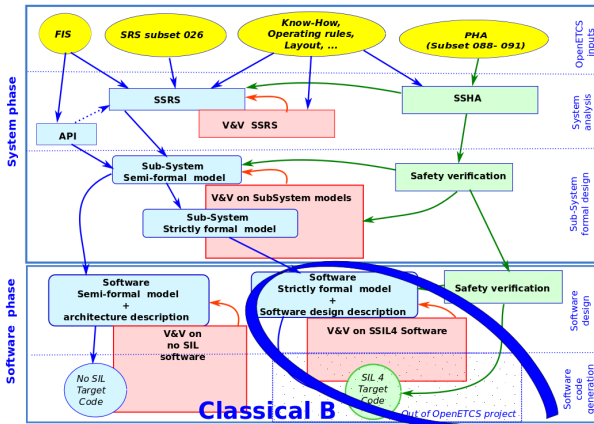
... to Y-cycle

In OpenETCS process

In OpenETCS process

Benchmark activities

- few elements of models (§3.5)
- no assessor
- documents to produce

Results of benchmark

- - Subset 26 is not adapted as input of software development
- - Elements to define software architecture not available (API, interface definition,...)
- + Well adapted to design software model
- + Structured and modular approach
- + Suitable to generate code
- + Formal verification means

Systerel

Tool

AtelierB (Clearsy) :

- ▶ usage accepted in several industrial process
- ▶ close source (except API) but free
- ▶ interactive or batch mode
- ▶ contents :
    - ▶ editor
    - ▶ checker : types, syntax,...
    - ▶ proof generator
    - ▶ automatic and interactive prover
- ▶ extensions : animator, translator, SMT solvers,...

Summary

+ Mature approach
+ Well adapted to design critical software : from software informal specification to automatic code generation
+ Easy to maintain
+ Formal verification
+ Industrial approaches and tools adapted to EN50128 requirements
- Methodology and Know-how not shared
- Industrial tools are not open source
- To be mixed with a high level model : Semi-formal model or Event B

Systerel