

Combining Verification and Validation techniques

EJCP'13 short presentation

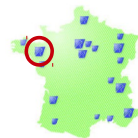
Erwan Bousse

IRISA, University of Rennes 1

May 25, 2013

Research group

- Triskell, at IRISA (University of Rennes 1)
- ~ 40 people
- Some topics:
 - Model Driven Engineering (MDE)
 - Models@Runtime
 - Requirements Engineering
 - Verification and Validation (V&V)
- Some tools:
 - Kermeta (model manipulation)
 - Kevoree (models@runtime)



Context: early V&V in Model Driven Developments

- **systems are more and more complex** (e.g. trains, cars, planes, satellites)
 - to cope with that, MDD and DSLs
 - need for V&V as early as possible
- how to perform *effective* V&V?

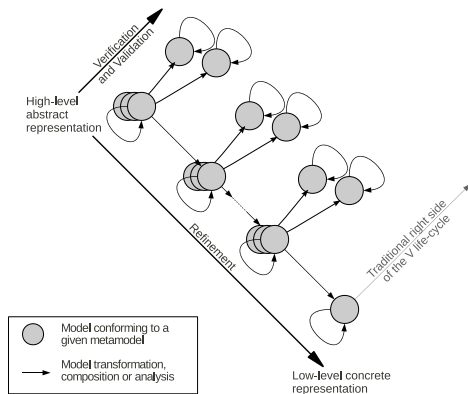


Figure: Left-hand side of the V life-cycle: V&V early and throughout

Problem studied: combining several V&V techniques

- **Many ways to perform V&V:** testing, model checking, theorem proving, runtime monitoring, static analysis, etc.
- Each technique has characteristics, e.g.:
 - **input languages** (level of abstraction, etc.)
 - **kinds of properties** they can prove (safety, liveness, etc.)
 - **coverage** (compliance for one/few/all execution trace(s))
 - **scalability** (small/big systems/properties)

→ many differences, thus different strengths and weaknesses

Idea: **Combining multiple V&V techniques**

Problems

- 1 Integration of V&V techniques
- 2 Semantic gap between DSLs and verification languages

Approach envisioned (1): modeling V&V evidence

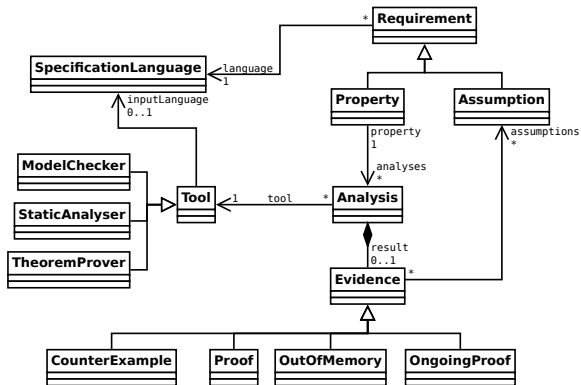


Figure: Intuitive framework to model V&V evidence and coverage, to share results between tools and integrate combined approaches

Approach envisioned (2): model typing

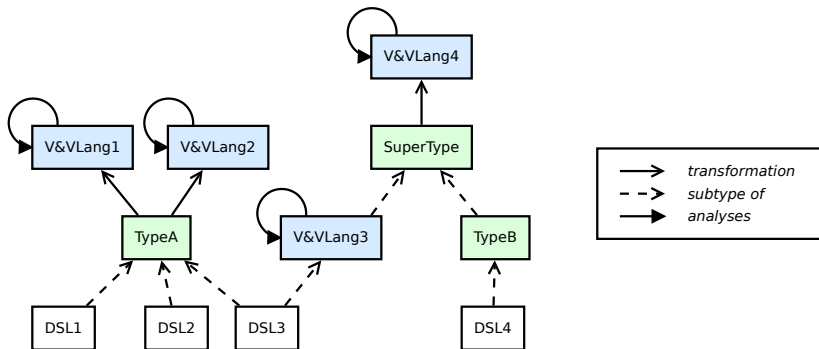


Figure: Capitalization of V&V analyses through model typing, to fill the semantic gap and reason about languages characteristics

Ongoing and future work

- **Ongoing work:** playing with a railway system use case
 - definition of a DSL and translations to V&V languages
 - trying to combine random testing and model checking
 - trying to define a framework draft and interesting model types
- **Long term goal:** a nice framework to facilitate the combinations of (some) techniques
- For more details: paper to be presented in ~ 1 month at ECMFA/ECOOP/ECSA'2013 Doctoral Symposium – PhD student workshop

Done!

Thank you! 😊

`erwan.bousse@irisa.fr`