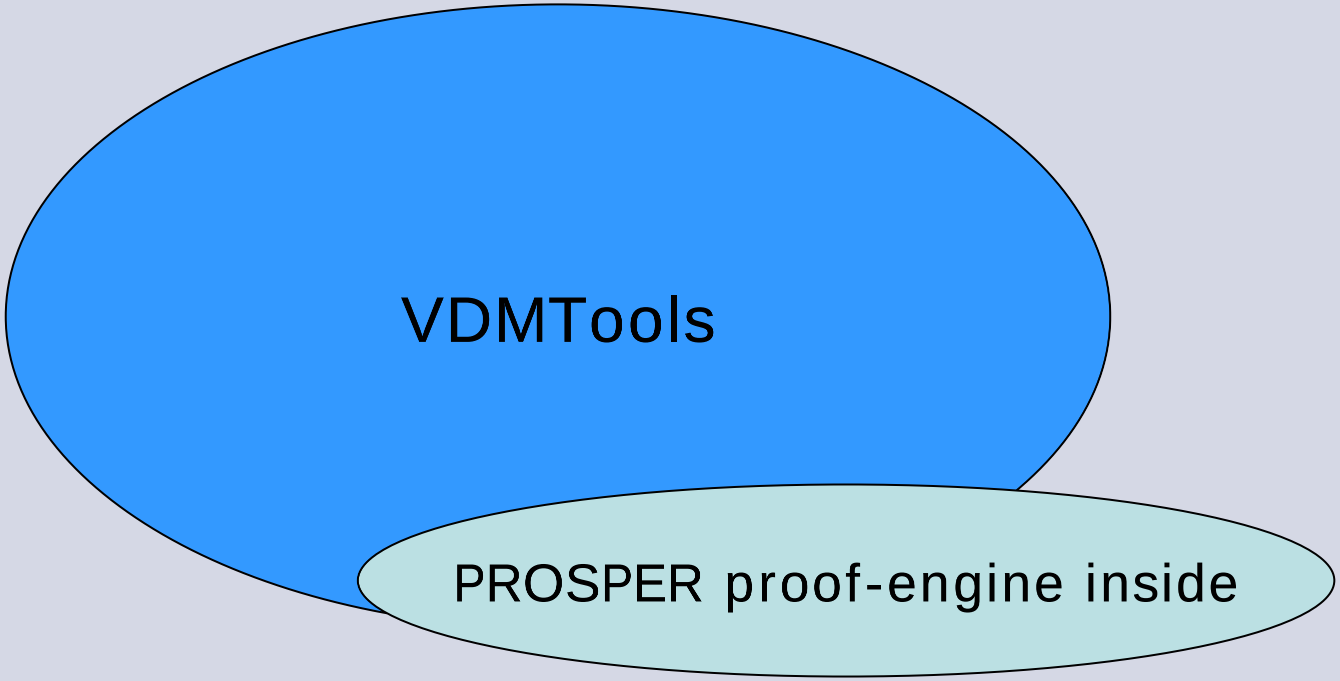
Getting PROSPER tool support usable again

Peter Gorm Larsen

PROSPER extensions



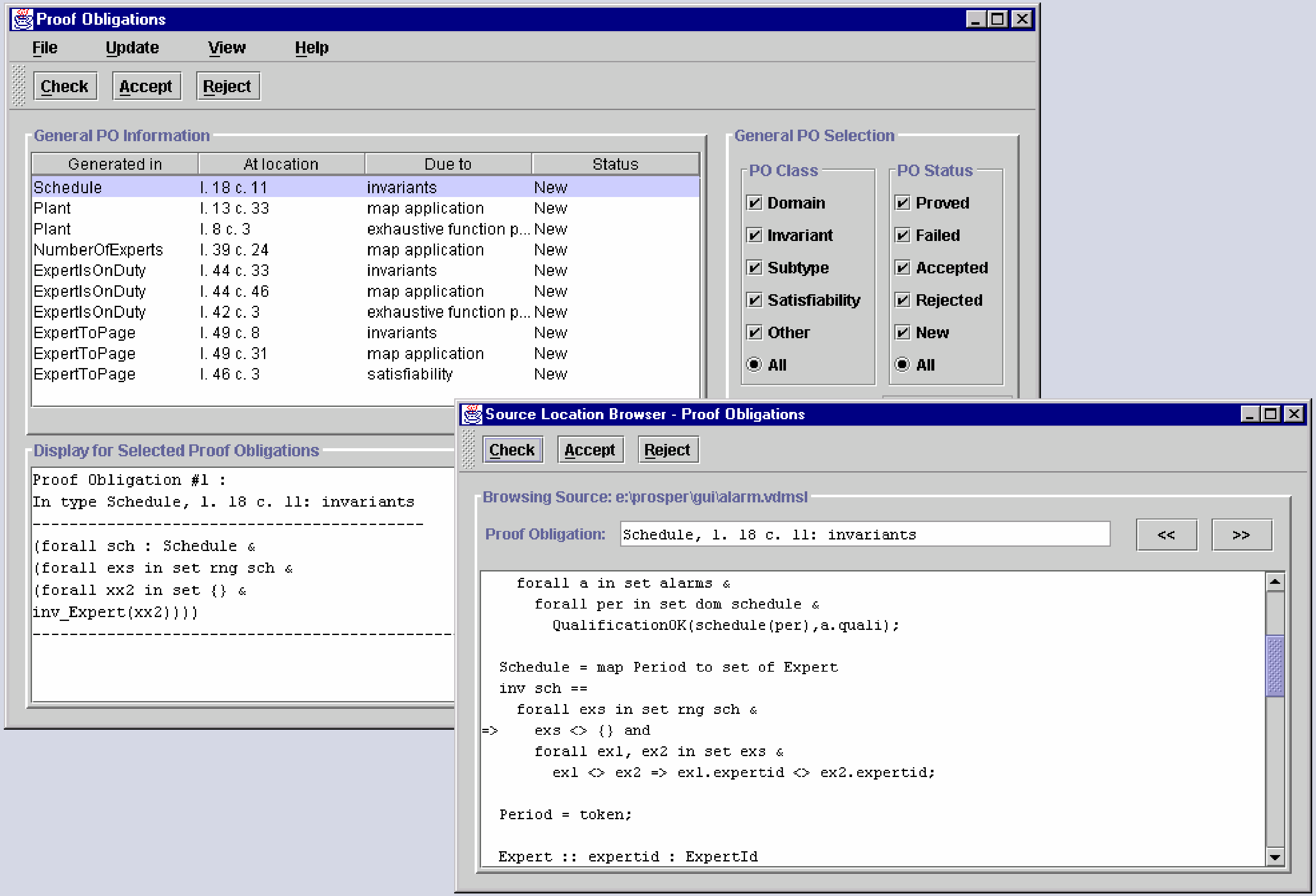
VDMTools

PROSPER proof-engine inside

PROSPER Case studies

- Alarm
- Tracker
- Safer
- Line database (RTRI)
- Interlocking (RTRI)

Proof obligation generator



General PO Information

Generated in	At location	Due to	Status
Schedule	l. 18 c. 11	invariants	New
Plant	l. 13 c. 33	map application	New
Plant	l. 8 c. 3	exhaustive function p...	New
NumberOfExperts	l. 39 c. 24	map application	New
ExpertIsOnDuty	l. 44 c. 33	invariants	New
ExpertIsOnDuty	l. 44 c. 46	map application	New
ExpertIsOnDuty	l. 42 c. 3	exhaustive function p...	New
ExpertToPage	l. 49 c. 8	invariants	New
ExpertToPage	l. 49 c. 31	map application	New
ExpertToPage	l. 46 c. 3	satisfiability	New

General PO Selection

PO Class
- ☑ Domain
- ☑ Invariant
- ☑ Subtype
- ☑ Satisfiability
- ☑ Other
- ● All

PO Status
- ☑ Proved
- ☑ Failed
- ☑ Accepted
- ☑ Rejected
- ☑ New
- ● All

Display for Selected Proof Obligations

```
Proof Obligation #1 :
In type Schedule, l. 18 c. 11: invariants
-------------------------------------------
(forall sch : Schedule &
(forall exs in set rng sch &
(forall xx2 in set {} &
inv_Expert(xx2))))
----------------------------------------------
```

Browsing Source: e:\prosper\gui\alarm.vdmsl

Proof Obligation: Schedule, l. 18 c. 11: invariants

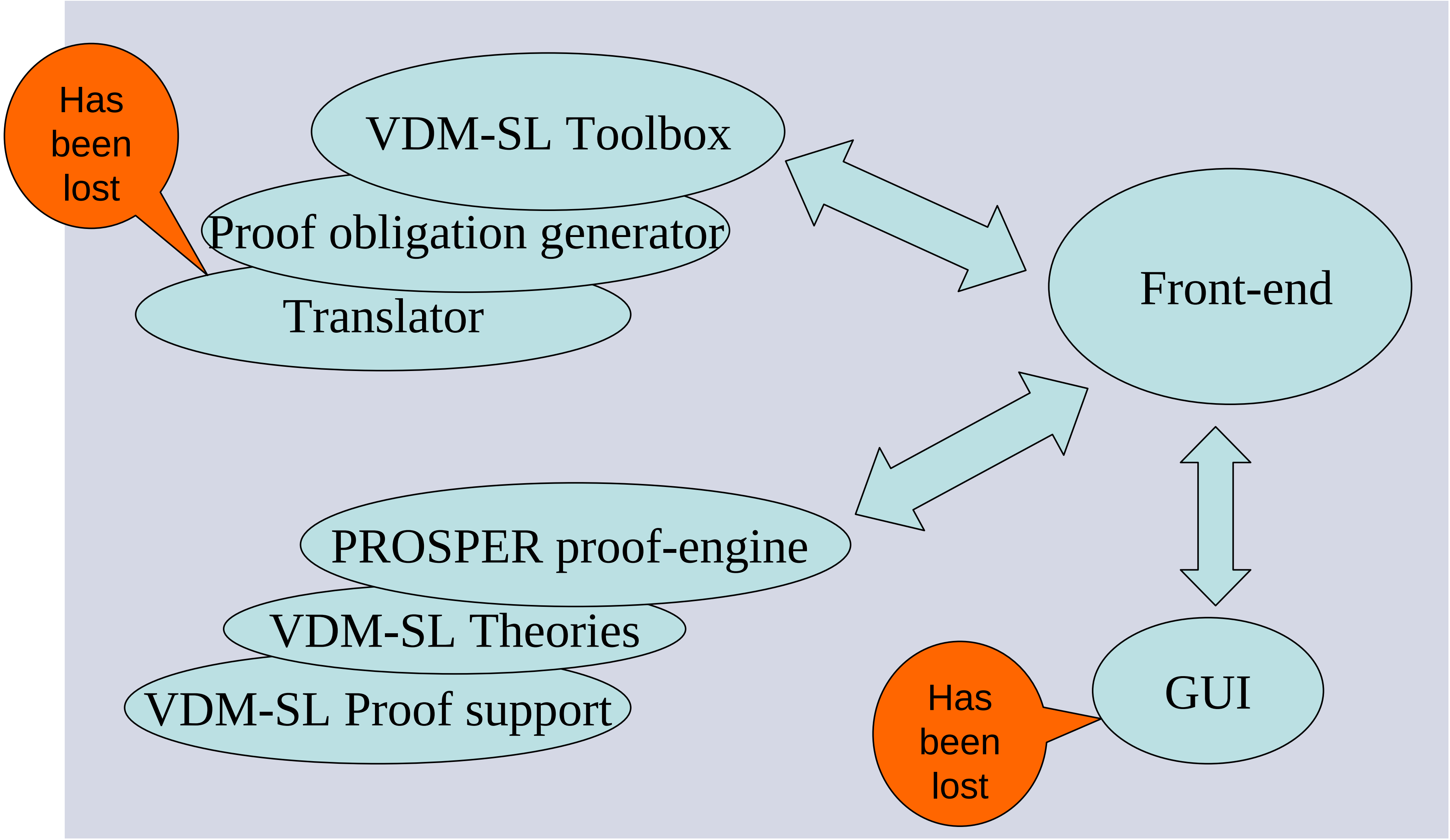
```
    forall a in set alarms &
      forall per in set dom schedule &
        QualificationOK(schedule(per),a.quali);

  Schedule = map Period to set of Expert
  inv sch ==
    forall exs in set rng sch &
=>    exs <> {} and
      forall ex1, ex2 in set exs &
        ex1 <> ex2 => ex1.expertid <> ex2.expertid;

  Period = token;

  Expert :: expertid : ExpertId
```

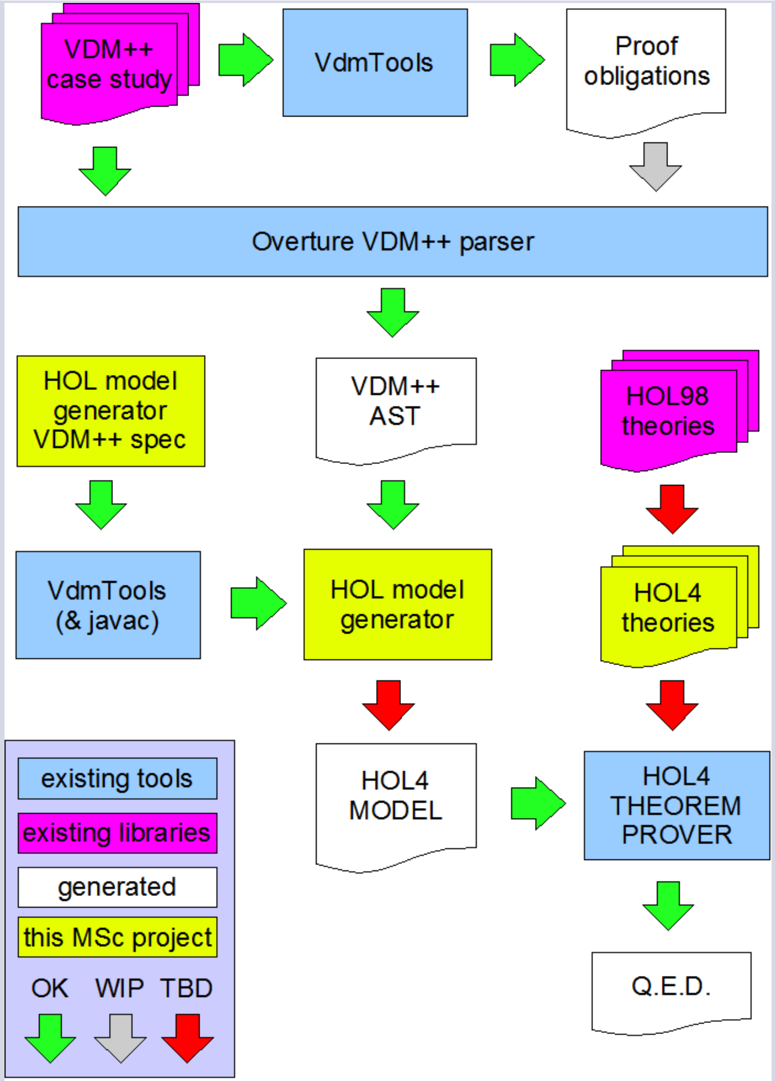
PROSPER Component View



Documents saved in hardcopy

- VDM-SL Toolbox extensions
- Proof-enabled VDM-SL Toolbox – release 2
- VDMTools: The Integrity Examiner
- Formalizing a subset of VDM-SL in HOL
- Reasoning about VDM-SL Proof Obligations in HOL
- A Two-valued subset of VDM-SL
- Translating a bounded subset of VDM-SL to Propositional Logic
- Translating Specifications in VDM-SL to PVS
- An Isabelle-based Theorem Prover for VDM-SL

New MSc project for Sander Vermolen



Tasks to do to revive PROSPER

- Get HOL theories and tactics upgraded to newest HOL
- Specify a translation between VDM and HOL
- Re-verify the VDM models inside HOL4
- Create a new GUI for proofs at VDM level
- Enable a combination of interactive and automatic proofs
- Enable model-checkking for a subset of VDM