

Automated Property Verification for Large Scale B Models



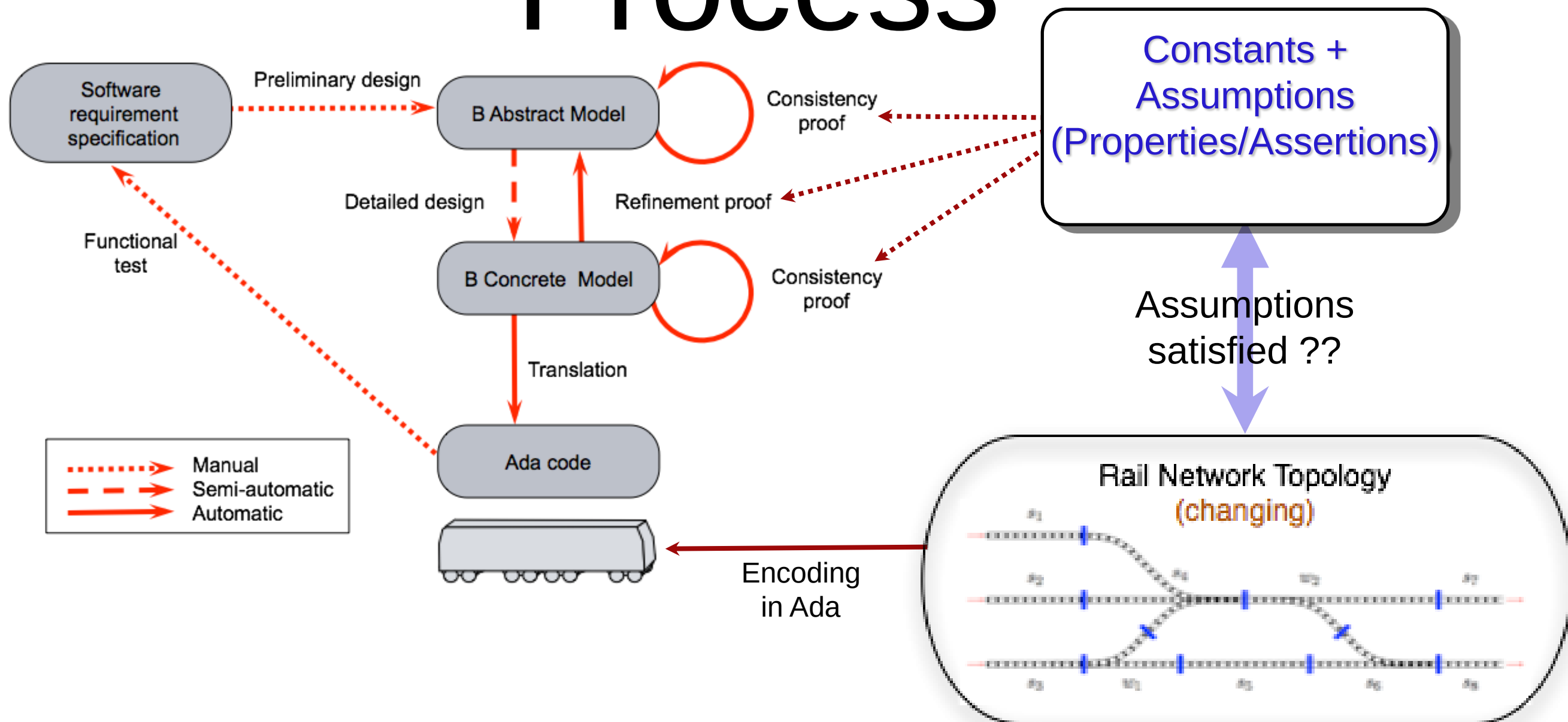
Jérôme Falampin (Siemens - STS)
Michael Leuschel, Fabian Fritz, Daniel Plagge
(Düsseldorf)



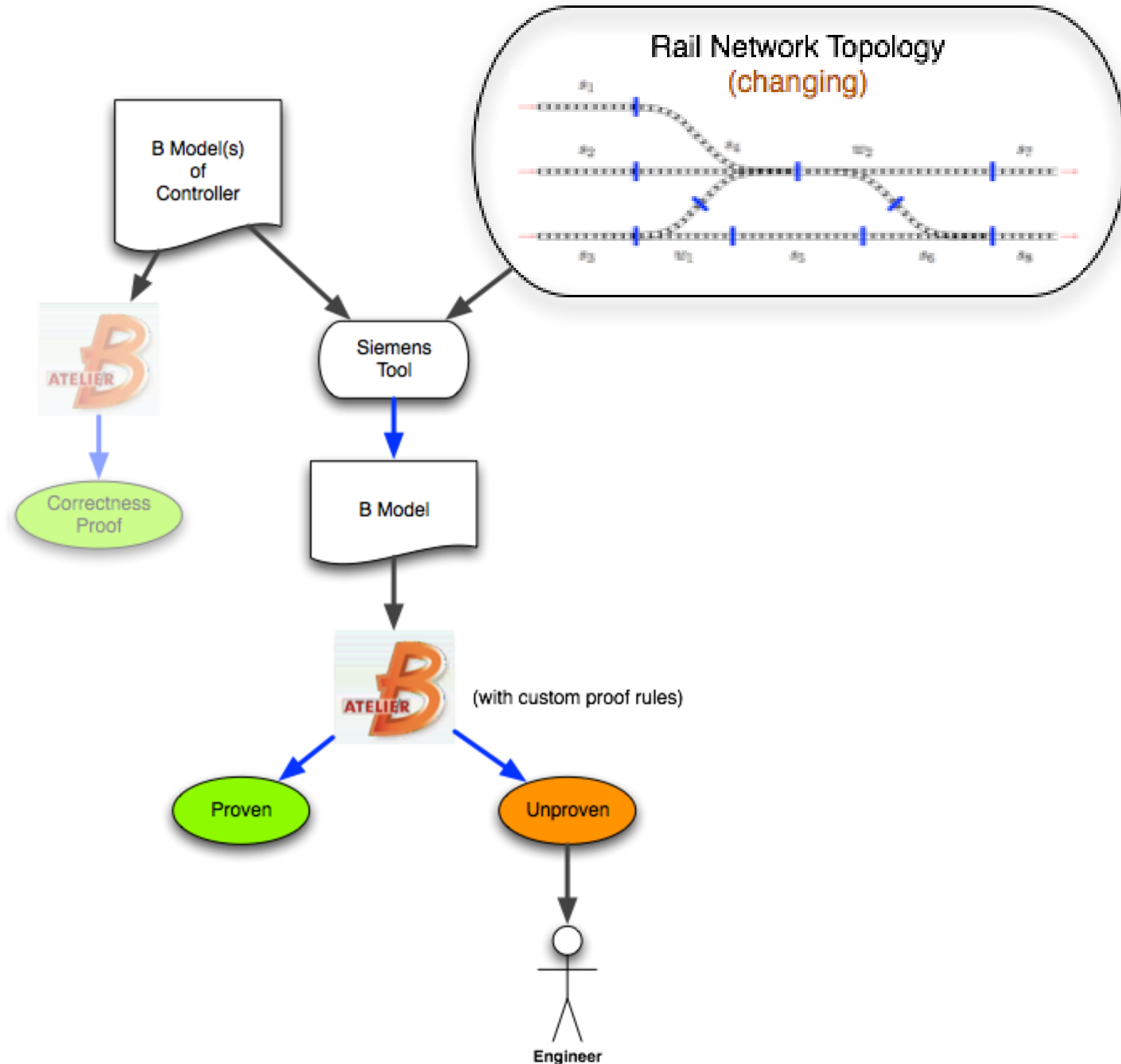
SIEMENS



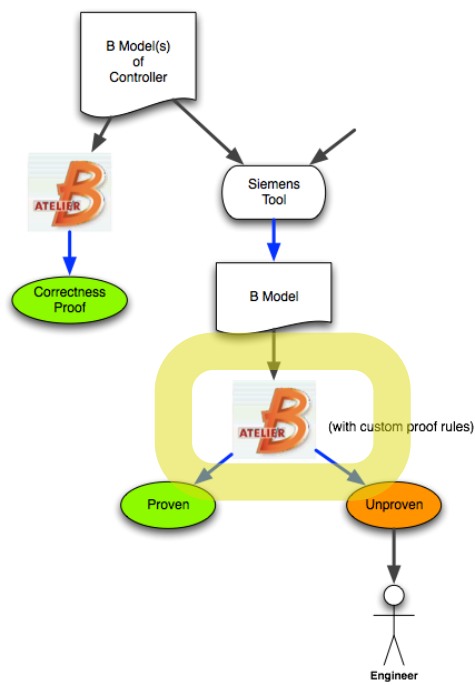
B Development Process



Validating Constants : Current Process



Problem



- AtelierB prover unable to deal with a considerable number of assertions
- Manual Inspection
 - large time & cost
 - problems found only very late



Enter



Prolog Core of ProB

7	8	1	6	3	2	9	4	5
9	5	2	7	1	4	6	3	8
4	3	6	8	9	5	7	1	2
2	4	9	3	7	6	8	5	1
6	7	3	5	8	1	2	9	4
5	1	8	4	2	9	3	6	7
1	9	4	2	6	7	5	8	3
8	6	7	1	5	3	4	2	9
3	2	5	9	4	8	1	7	6

- ProB kernel
 - “constraint solver” over B’s datatypes
- ProB interpreter for B/Event-B
 - predicates
 - expressions
 - substitutions

Can we use this
to validate the
assumptions ?



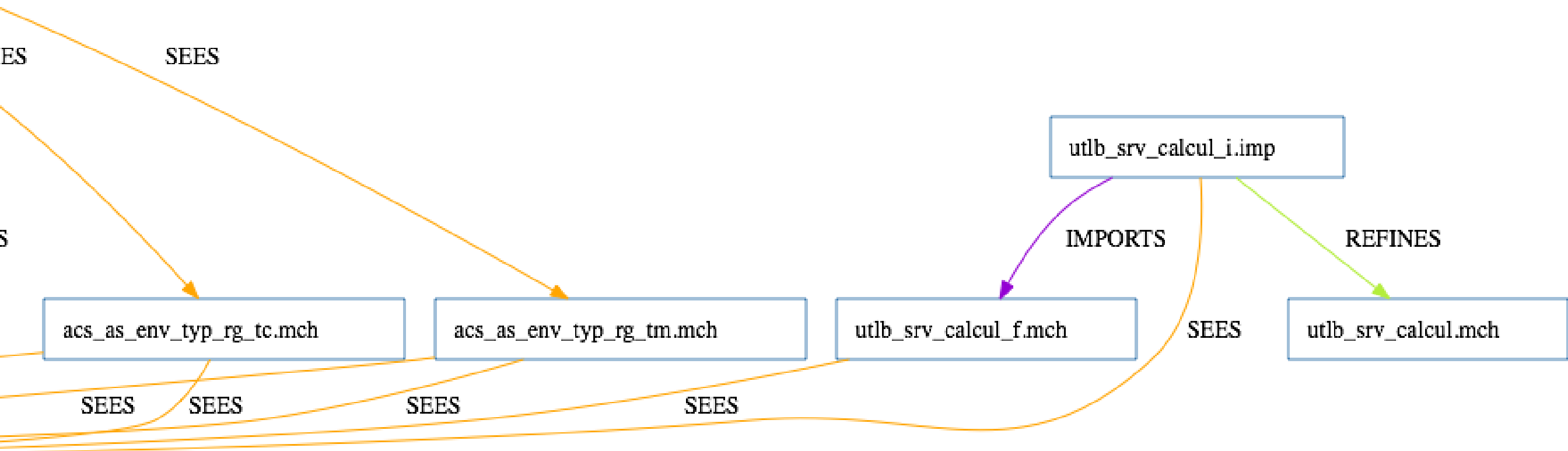
San Juan Case Study



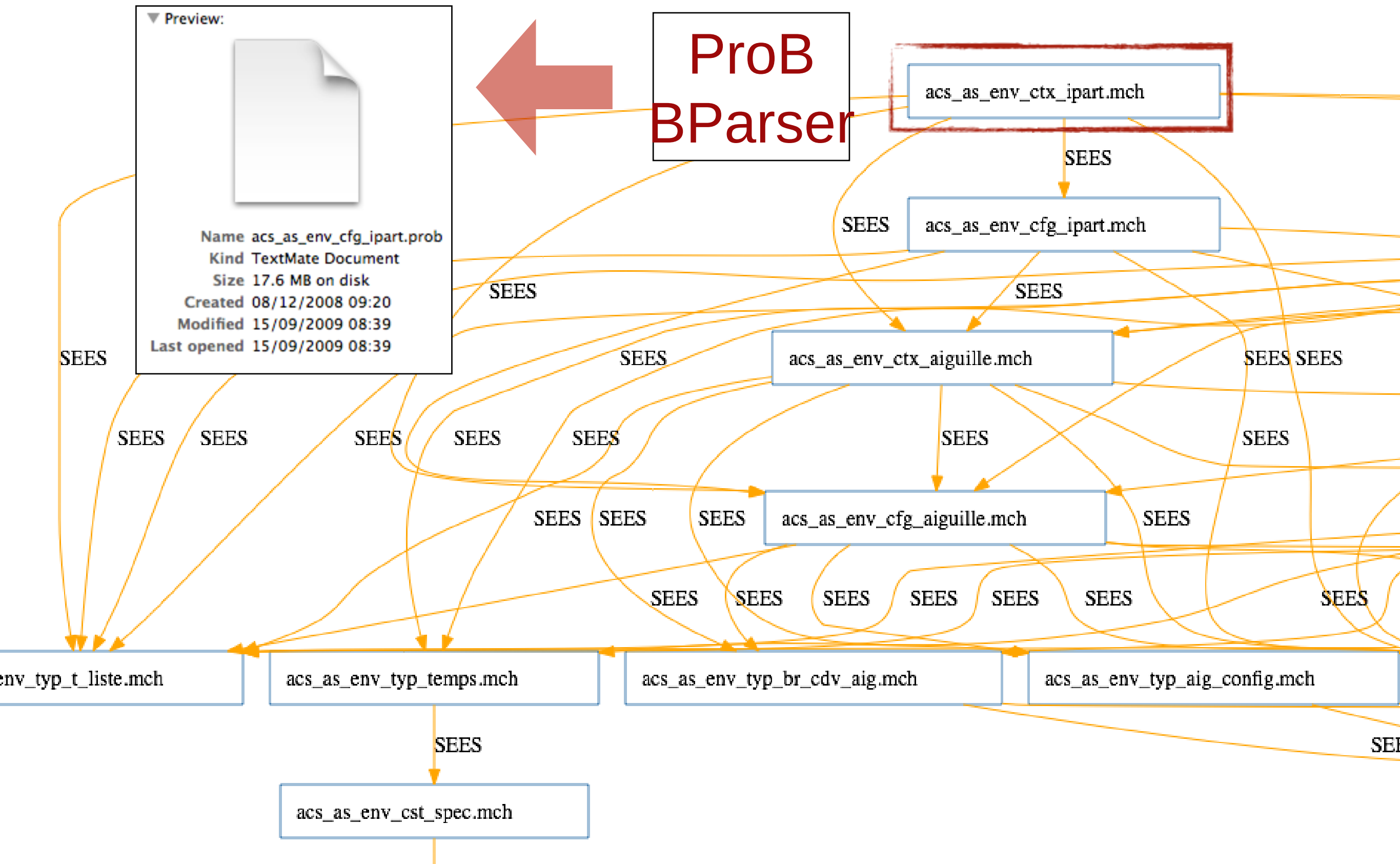
- 142 constants, up to 2324 tuples
- 226 properties (concrete constants + glueing properties for abstract constants)
- 147 assertions (real assumptions)
- 80 assertions could not be checked by AtelierB (out of memory)

Module Hierarchy

79 files
>23,000 lines of B



Module Hierarchy



Some of the 147 Assertions

```
!(aa,bb).(aa:t_iti_partiel_acs & bb:cfg_cdv_aig & aa |->  
          bb:t_iti_partiel_acs <|  
          cfg_ipart_cdv_transit_dernier_i |> cfg_cdv_aig =>  
          bb:cfg_ipart_cdv_transit_liste_i[  
(cfg_ipart_cdv_transit_deb(aa)..cfg_ipart_cdv_transit_fin(aa))])
```

```
dom({aa,bb|aa:t_aig_acs & bb:t_cdv_acs &  
bb:cfg_aig_cdv_encl_liste_i[(cfg_aig_cdv_encl_deb(aa) ..  
cfg_aig_cdv_encl_fin(aa))]) = t_aig_acs
```

```
ran({aa,bb|aa:t_aig_acs & bb:t_cdv_acs &  
bb:cfg_aig_cdv_encl_liste_i[(cfg_aig_cdv_encl_deb(aa) ..  
cfg_aig_cdv_encl_fin(aa))])  
= cfg_cdv_i~[{c_cdv_aig}]
```

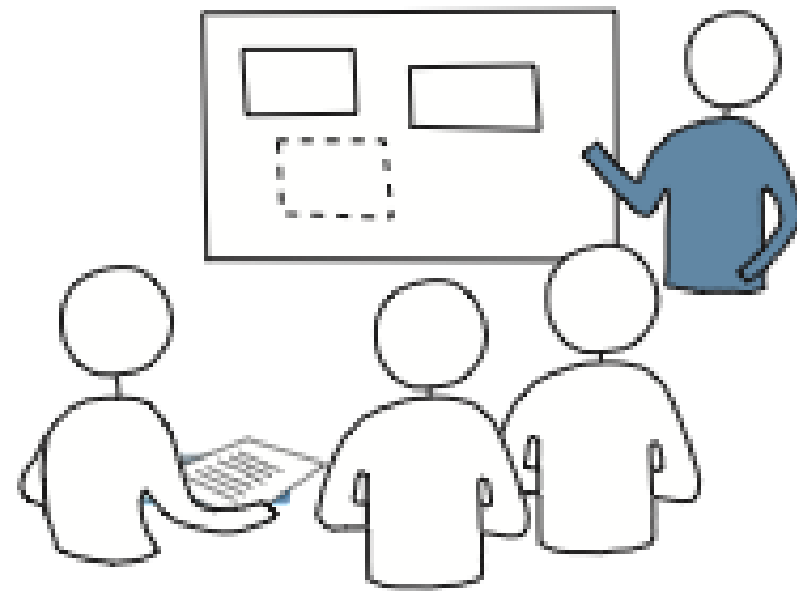


80

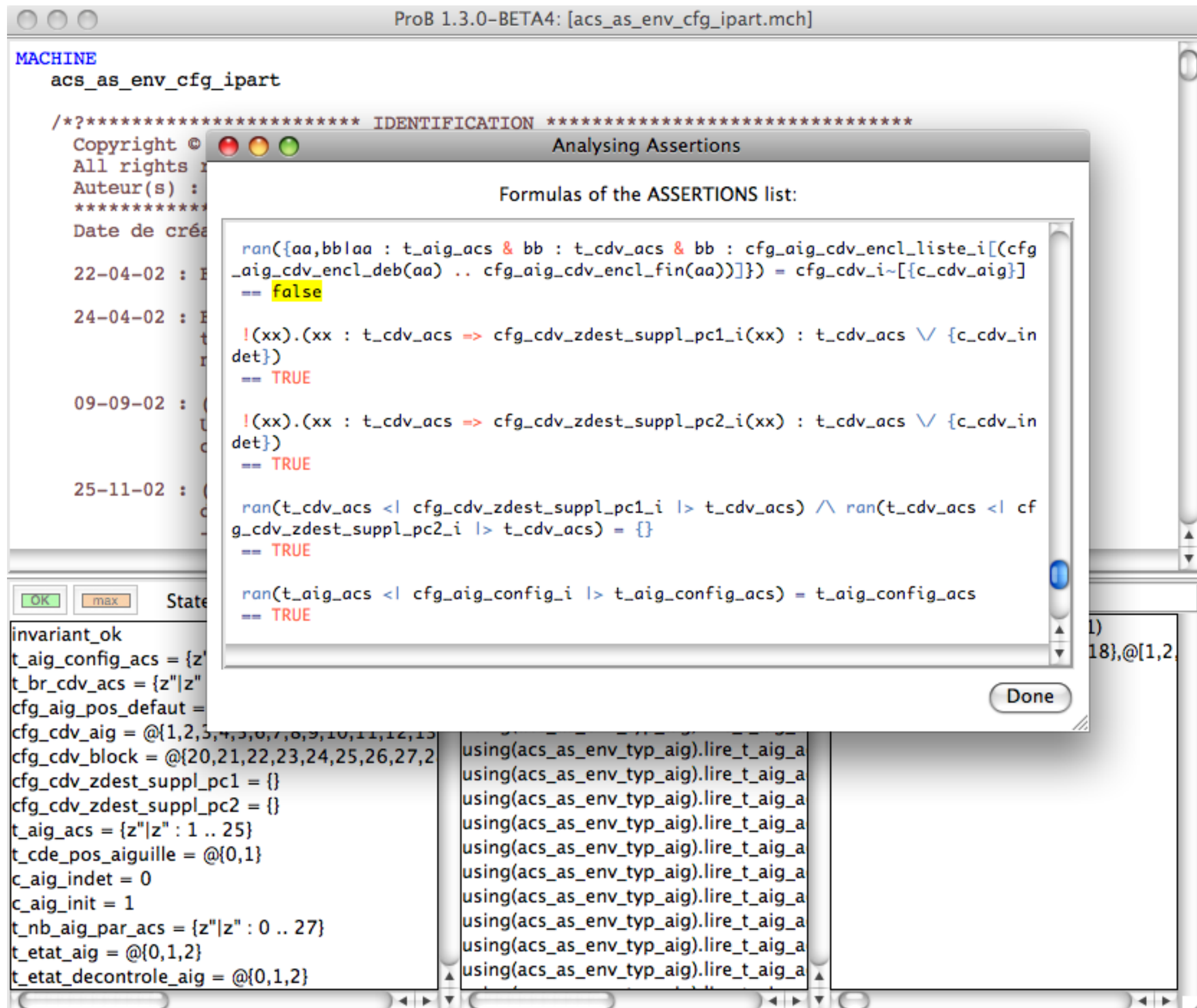
Properties/Assertio
ns

+/- 1 Man Month !

Manual Inspection by Siemens



After 3 min 17 seconds





Result of Case Study

- Further improvements to ProB required (as outlined in earlier presentation)
- Four false assumptions were found
 - 1 Property, 3 Assertions
 - exactly same problems found by manual inspection (and issues were corrected)
- Formula Viewer of ProB useful to identify sources of inconsistency

Next Steps

Validation

(Even)
Bigger Models

Deployment

PAL - Paris Line 1

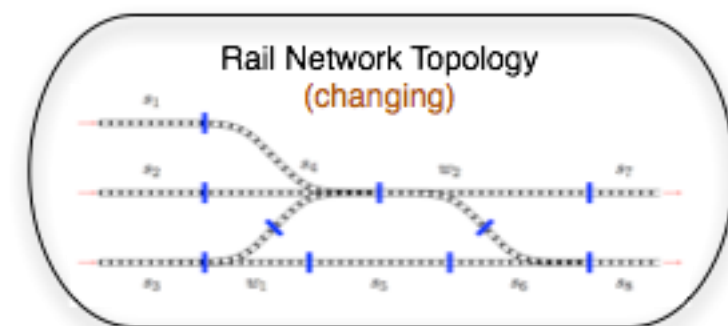


- 74 Files, >10,000 lines of B
- +/- 2000 Assertions to be checked
- Again all problems found (12) in under 5 minutes
- No false alarms

Two more components to go



Summary



- ProB can be used to validate large B models with real-life data
- Two experiments (San Juan, Paris Line 1):
 - 1 Man Month of Work $\Rightarrow$ < 5 minutes
 - Better Feedback
- Siemens plans to deploy ProB in SIL-4 chain
- Useful for other applications (SAP,...)



Thanks !

- Jens Bendisposto
- Carl Friedrich Bolz
- Nadine Elbeshausen
- Fabian Fritz
- Marc Fontaine
- Stefan Hallerstedde
- Michael Jastram
- Li Luo
- Daniel Plagge
- Mireille Samia
- Corinna Spermann
- Dennis Winter



- Michael Butler
- Thierry Massart
- Edd Turner



SIEMENS

