systerel
Solutions temps réel sécurisées

Systerel Smart Solver
InnoTrans – openETCS

Sept 2014

S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

Systerel Smart Solver

systerel
Solutions temps réel sécurisées

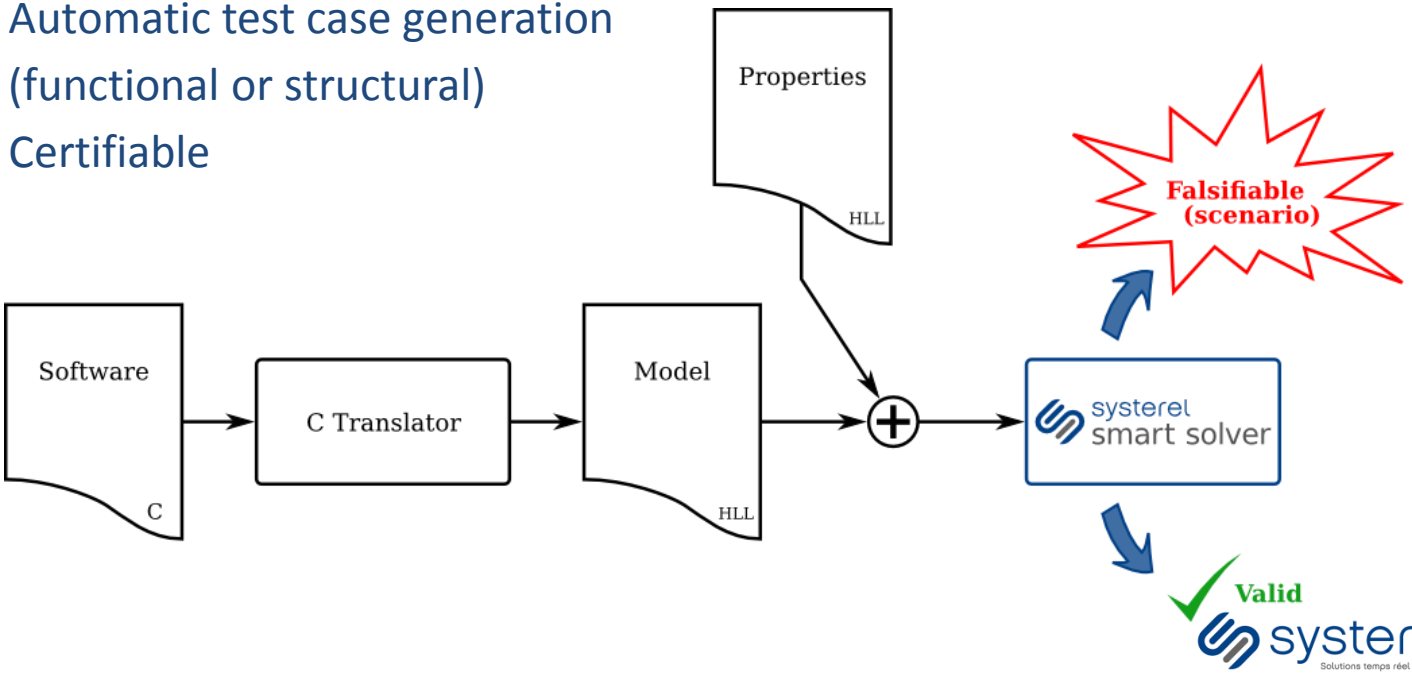
Systerel Smart Solver

- Family of « Model Checking » solutions
- SAT based – largely automatic
- Large application spectrum:
  - Property proofs – Certification
  - Absence of unspecified code behavior
  - Automatic test case generation (functional/structural)
  - Equivalence proofs
  - Extended debugging – simulation
  - Constraints satisfaction, optimizations, routing, planning, …
- Languages to express models and properties (HLL, sHLL)
- Generic toolset proven in use on industrial size systems
- Specialized translators (C, Ada, Scade, …)
- Team of experts (support, consulting, specific solutions, …)

S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

Systerel Smart Solver for C

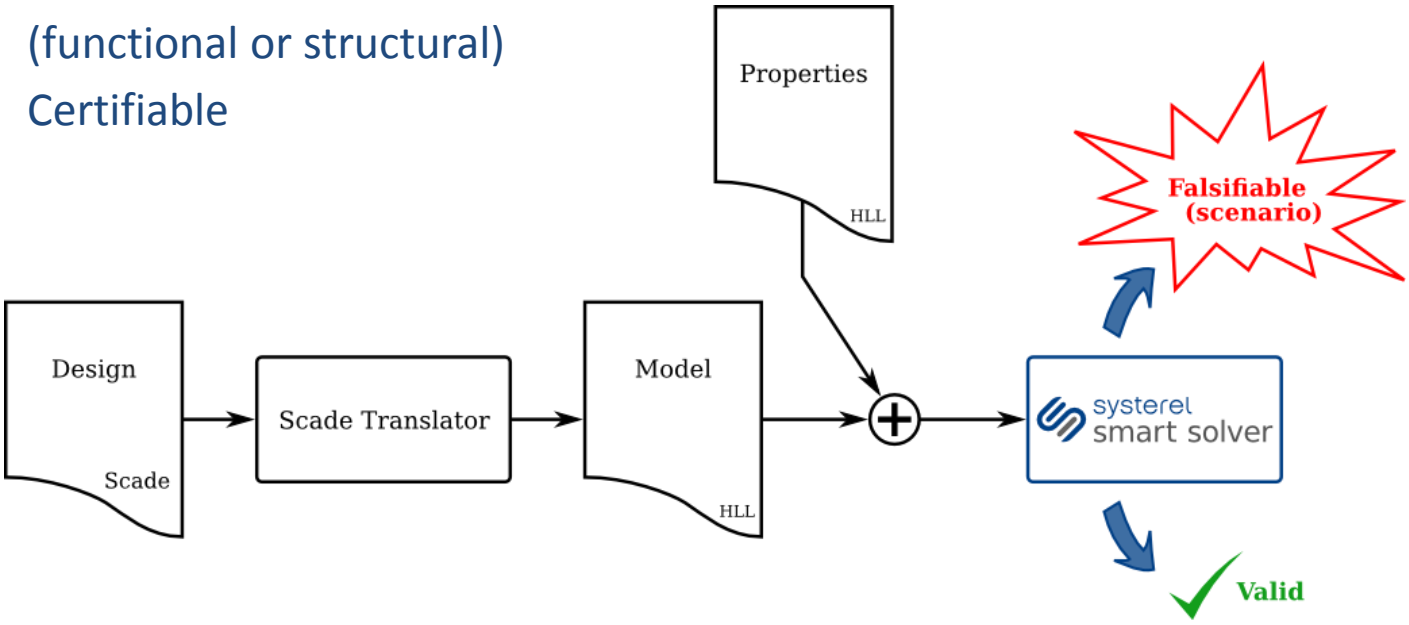
- Static analysis of C code (C99 with some restrictions)
- Exact modeling (no abstractions)
- Analysis of user-defined properties
- Analysis of unspecified behaviors (out of bond accesses, overflows, uninitialized variables, unreachable code, dead code, …)
- Automatic test case generation (functional or structural)
- Certifiable



S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

Systerel Smart Solver for Scade

- Static analysis of Scade designs (v5 and v6)
- Exact modeling (no abstractions)
- Analysis of user-defined properties
- Analysis of unspecified behaviors (overflows, uninitialized variables, …)
- Automatic test case generation (functional or structural)
- Certifiable

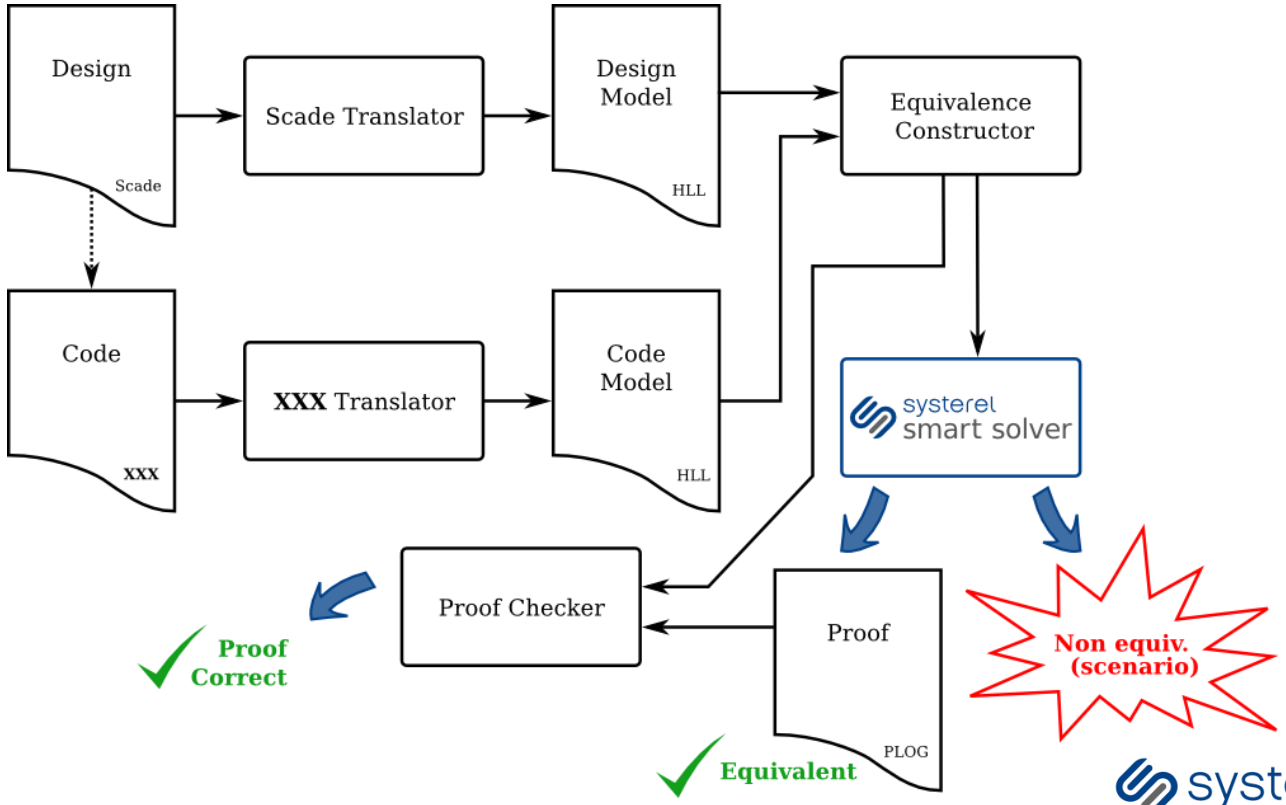


S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

systerel
Solutions temps réel sécurisées

Systerel Certifiable Smart Solver for Scade

- Certifiable analysis of Scade designs (v5 and v6)
- T2 SIL-4 EN 50128:2011, on-going for DO178
- Diversification, sequential equivalence checking, proof verifications



S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

Systerel Smart Solver for openETCS

- Basically, a solution based on “S3 for Scade”
- First attempt on a partner Scade model: train position computation
  - show conformance with the openETCS specification
  - difficult because it has its own specification (interpretation of the openETCS specification)
  - a few safety properties written
  - will most probably fail

- Systerel will develop a Scade model of part of the specification
  - level modes and transitions
  - mainly automaton based
  - strict conformance with the openETCS specification
  - proof of safety properties on this model
  - will also use certification

S3
S3 for C
S3 for Scade
cS3 for Scade
S3 for openETCS
Contact

Continue the discussion…

- S3
- S3 for C
- S3 for Scade
- cS3 for Scade
- S3 for openETCS
- Contact

Visit us at our InnoTrans booth 11.2-110N