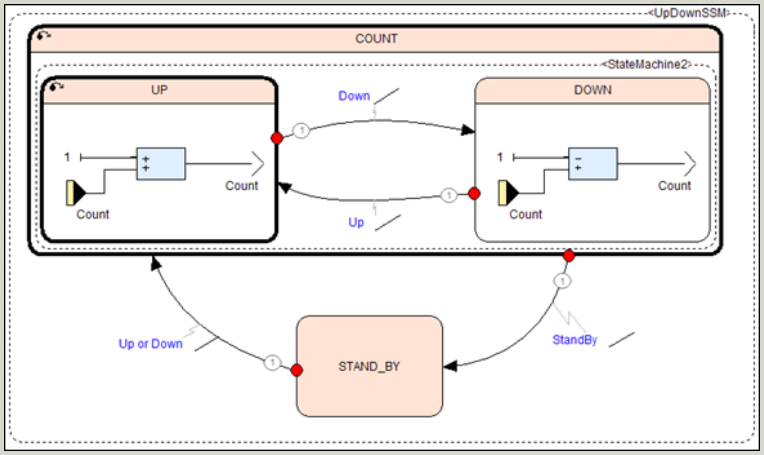
SIEMENS

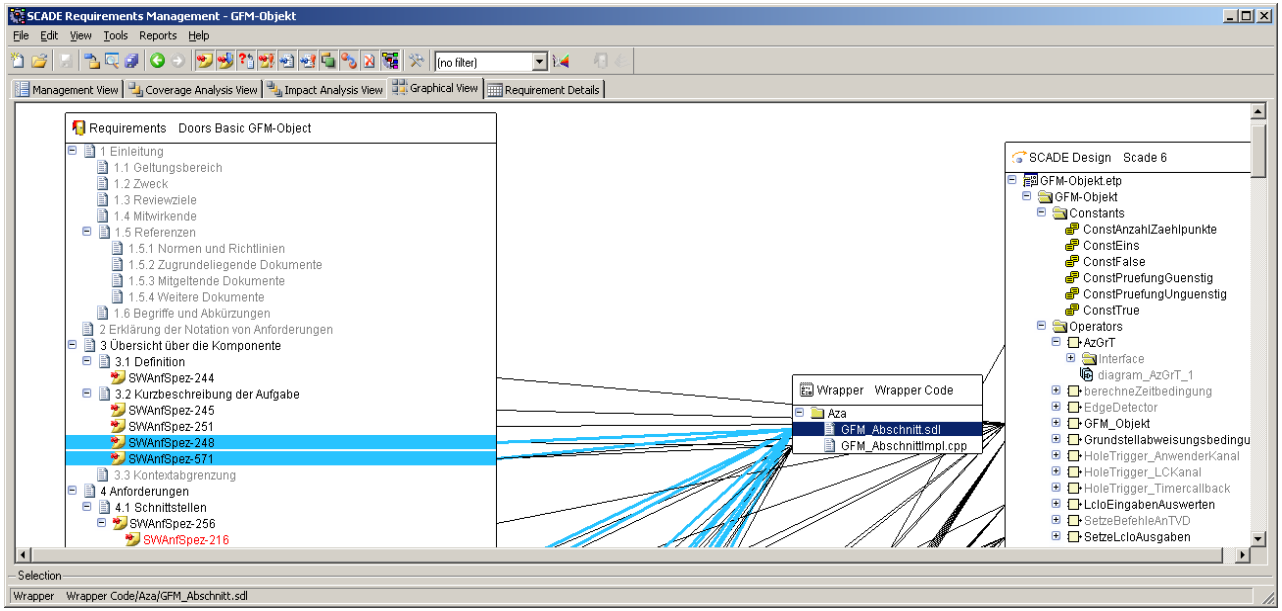


openETCS: WP 7 Model and Tool Evaluation
Subset 26, Sect. 3.5 (Management of Radio Communication)

Modelling „Management of Radio Communication“ with SCADE

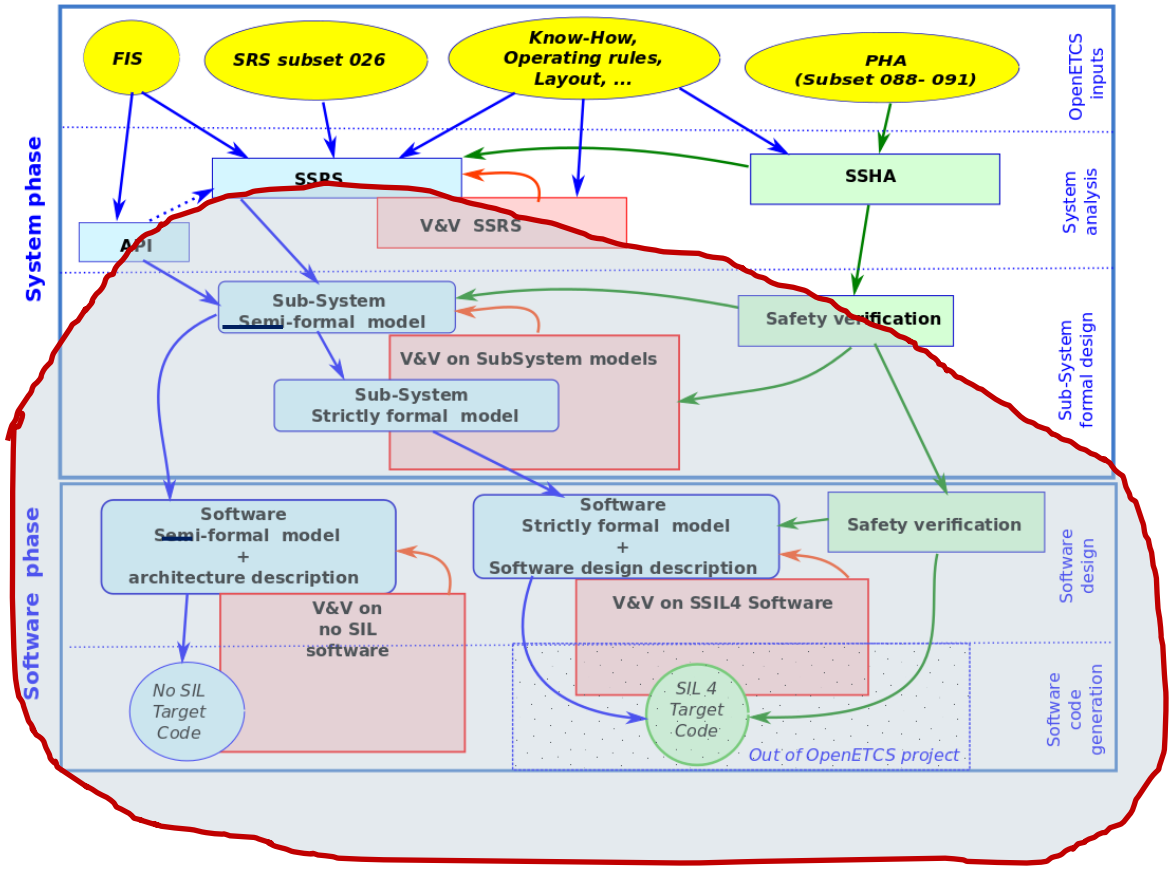
Agenda

- SCADE language and tool suite
- MoRC model (Management of radio communication)
- Results and actual status
- Next steps



SCADE Suite:
addresses especially
safety-related software (DO-178B, EN 50128 SIL 4)

SIEMENS

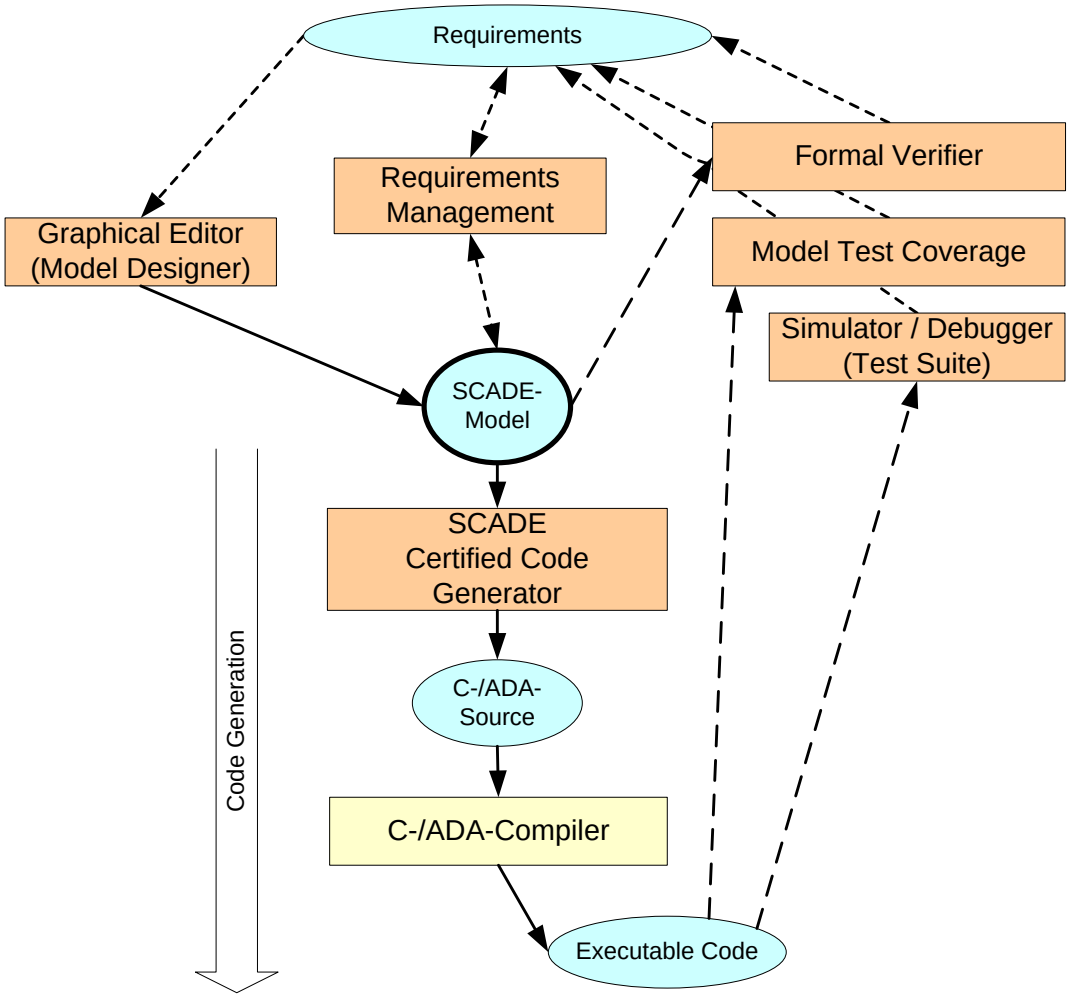


The SCADE Suite covers ...

... many aspects of the openETCS process

SCADE Suite: addresses especially safety-related software (DO-178B, EN 50128, SIL 4)

SIEMENS



What is SCADE?

- Modelling language and engineering platform from Esterel Technologies
- Model design, test and verification
- Requirements management gateway
- Automatic code generation
- Semantic checks during generation
- Certified code generator
- Debugging + simulation
- Formal Verifier
- Model test coverage

The SCADE Paradigm

SCADE Language

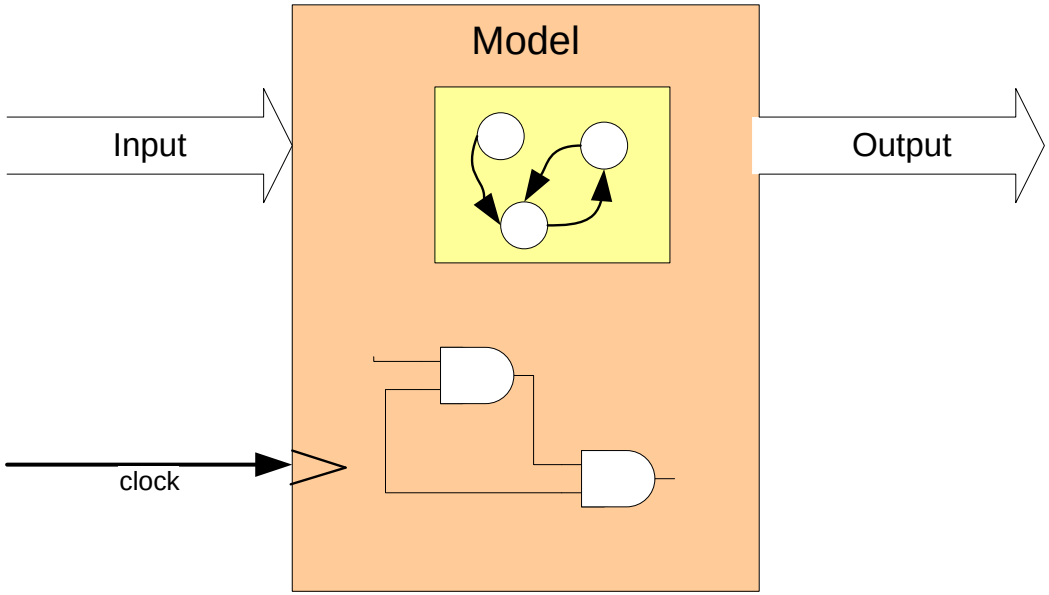
- Strictly formal and deterministic

SCADE-Models are

- synchronously
- clocked
- data flow and state machines
- combinations of these

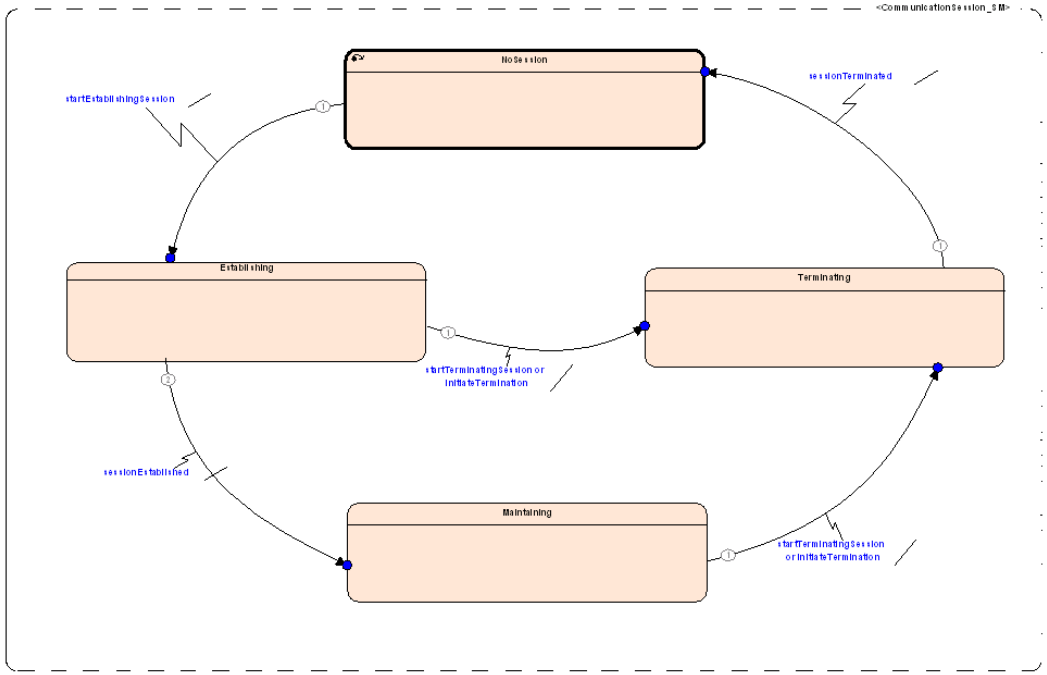
Timing Behavior

- no signal racing effects
- no transient bug effects



Management of Radio Communication

- Subset 026, 3.5:
  - ≈ 60 textual requirements on 10 text pages
  - 4 sequence charts
  - 3 tables
- Function:
  - Session Management



Actual Status

SIEMENS

- Formalization of the Spec (Modelling): Done
  (only few very ambiguous requirements left over)
- Executable C code generation: Done
- Model documentation (hand written & generated reports): Done
- Requirements tracing (Textual spec ↔ Model): Done
- Interface to Cecile Braunstein's RT-Tester & SysML/EA model: Done
- Model is ready for debugging, testing and verification

MoRC Model + generated C-Code + documentation on github:

- https://github.com/openETCS/model-evaluation/tree/master/model/SCADE_Siemens

To be done

- Model debugging + Testing with SCADE Suite tools
- Implementing sample test cases as specified in Subset ...
- Model based testing of the SCADE model as the system-under-test, Cecile’s EA/SysML model as test model and RT-Tester as test environment
- Measuring model test coverage values
- Sample proving
-

Benefits & Weaknesses

SIEMENS

- ✓ The model is strictly formal and concrete.
- ✓ The model is the implementation.
- ✓ The model is executable, simulatable and verifiable.
- ✓ Code generator qualified for for safety-related software development compliant to DO-178B/Level A and CENELEC EN50128/SIL4
- ✓ Tools for requirements tracing, model test coverage, report generation, ... provided
- – Textual spec structure → model structure = formalized spec
  Cannot be expected to be an optimal implementation
- – For more complex systems a more abstract, less formal intermediate layer language like SysML reasonable between textual spec and SCADE