Using formal methods without knowing them

Francesco Tiezzi

DSIUF, Università di Firenze

Sensoria Meeting
Milan — November 23-25, 2009

Joint work with Federico Banti and Rosario Pugliese

Aim of this work

Enable verification of properties of service-oriented systems modelled by high-level (UML-based) modelling languages . . .

Aim of this work

Enable verification of properties of service-oriented systems modelled by high-level (UML-based) modelling languages . . .

. . . through the use of formal methods

Aim of this work

Enable verification of properties of service-oriented systems modelled by high-level (UML-based) modelling languages . . .

. . . through the use of formal methods

Formal methods

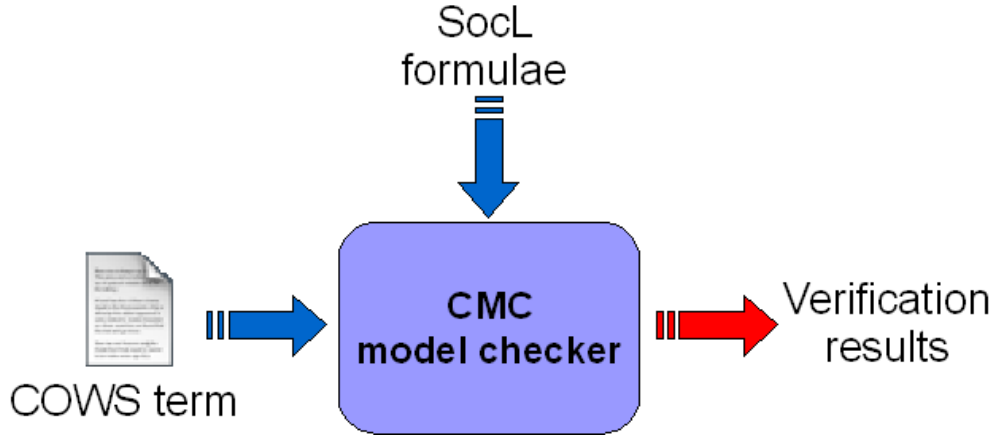
- Process calculi
- Temporal logics
- Model checking

Model checking: a calculus-based approach

- *Model checking* is a successful technique for verifying models of hardware and software systems

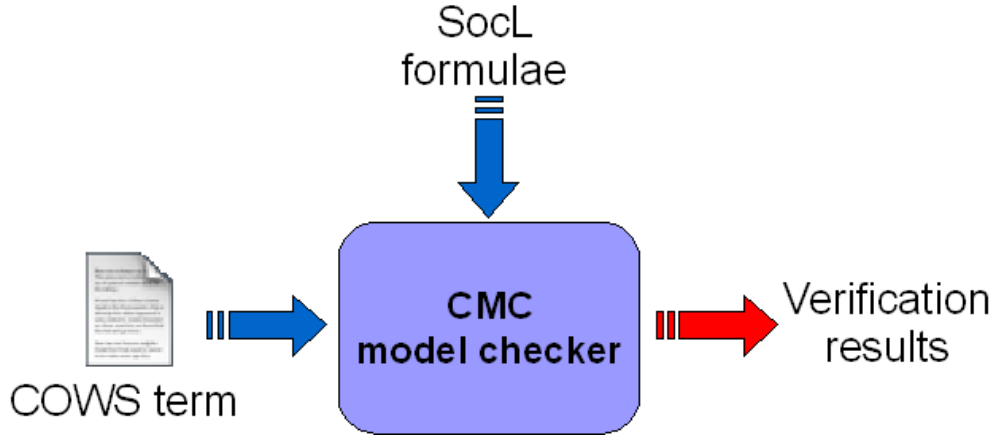
Model checking: a calculus-based approach

- *Model checking* is a successful technique for verifying models of hardware and software systems
- We have developed a calculus-based methodology for model checking COWS specifications (joint work of DSIUF and ISTI)



Model checking: a calculus-based approach

- *Model checking* is a successful technique for verifying models of hardware and software systems
- We have developed a calculus-based methodology for model checking COWS specifications (joint work of DSIUF and ISTI)



People in charge of verifying systems are required to understand and deal with calculi and logics.

This may not be the case, especially within industrial contexts

Model checking: a calculus-based approach

- *Model checking* is a successful technique for verifying models of hardware and software systems
- We have developed a calculus-based methodology for model checkin‹ of DSIUF and ISTI)

Just an example...

Verification results

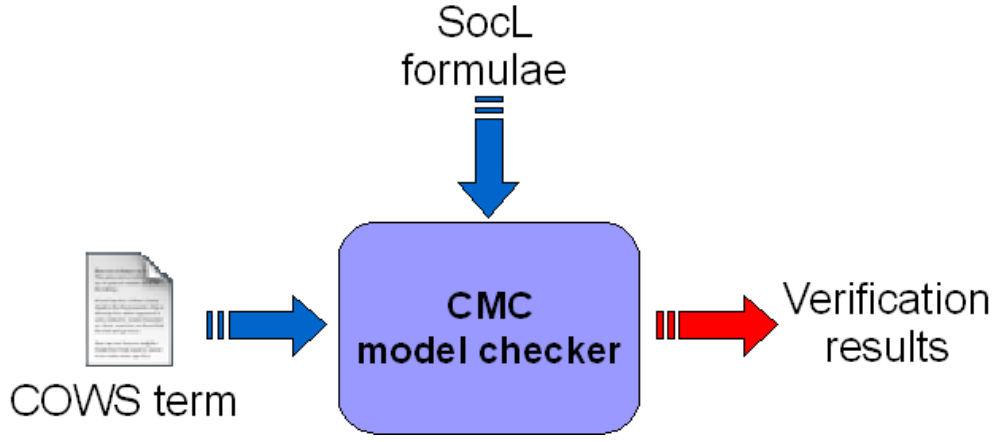
People in chai› understand and deal with calculi ar

This may not be the case, especially within industrial contexts

Information Society Technologies

Model checking: a calculus-based approach

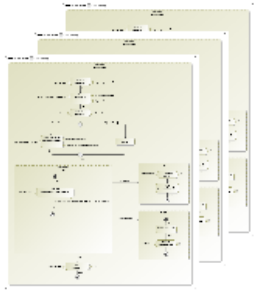
- *Model checking* is a successful technique for verifying models of hardware and software systems
- We have developed a calculus-based methodology for model checking COWS specifications (joint work of DSIUF and ISTI)



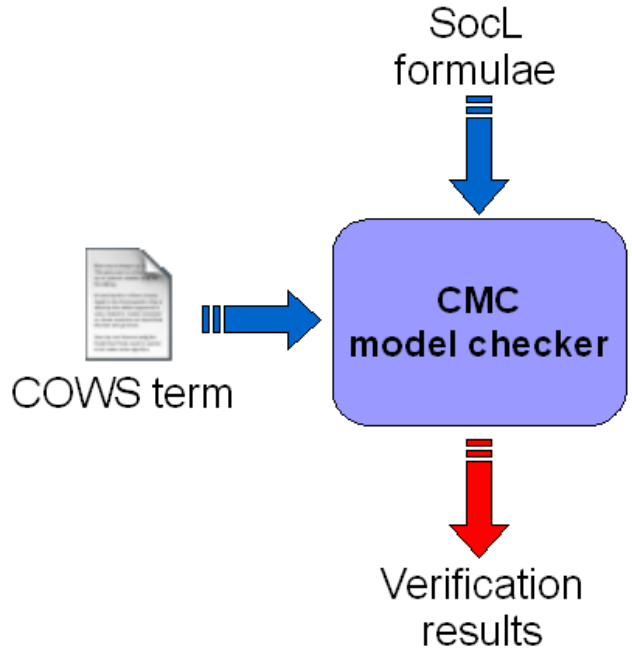
People in charge of verifying systems are required to understand and deal with calculi and logics.

This may not be the case, especially within industrial contexts, where people are usually familiar with higher-level UML-based modelling languages

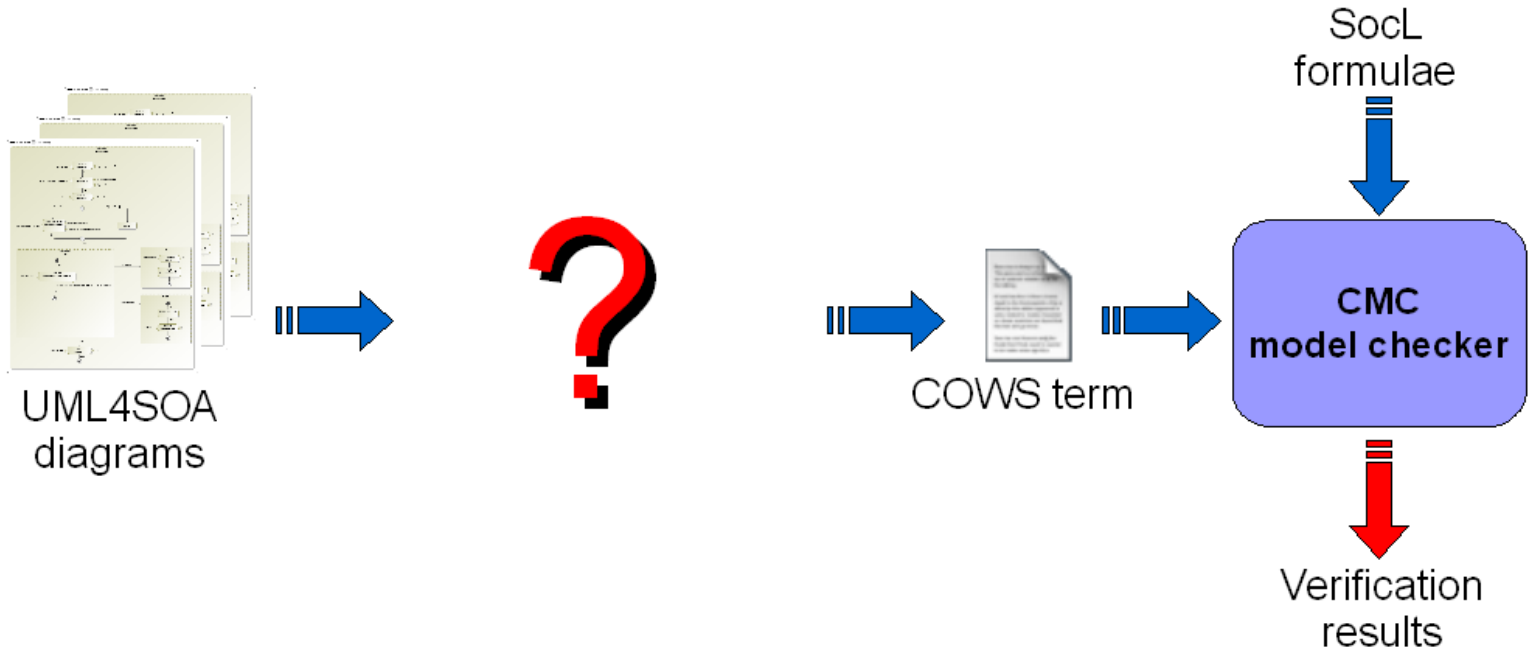
How to reconcile



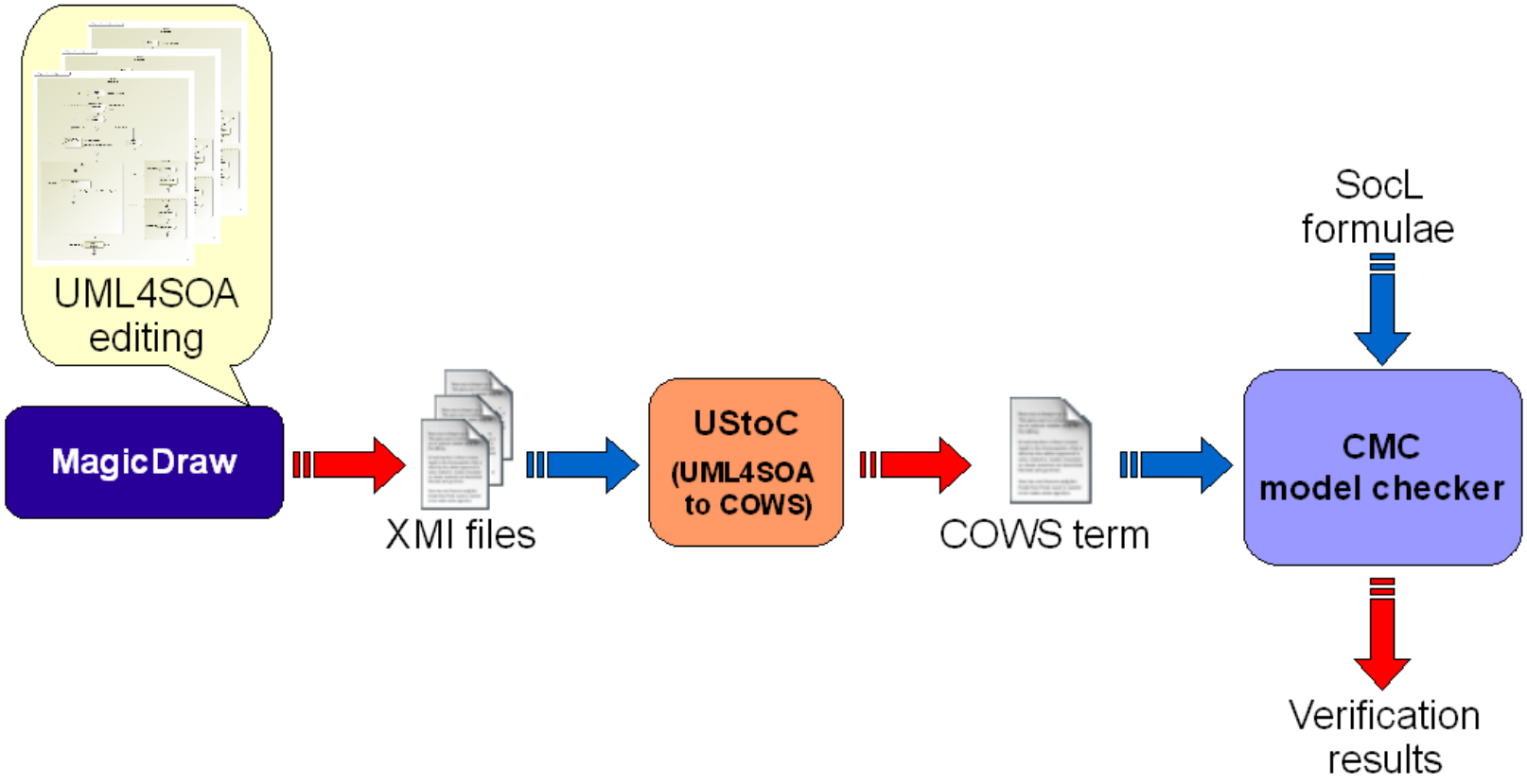
UML4SOA diagrams



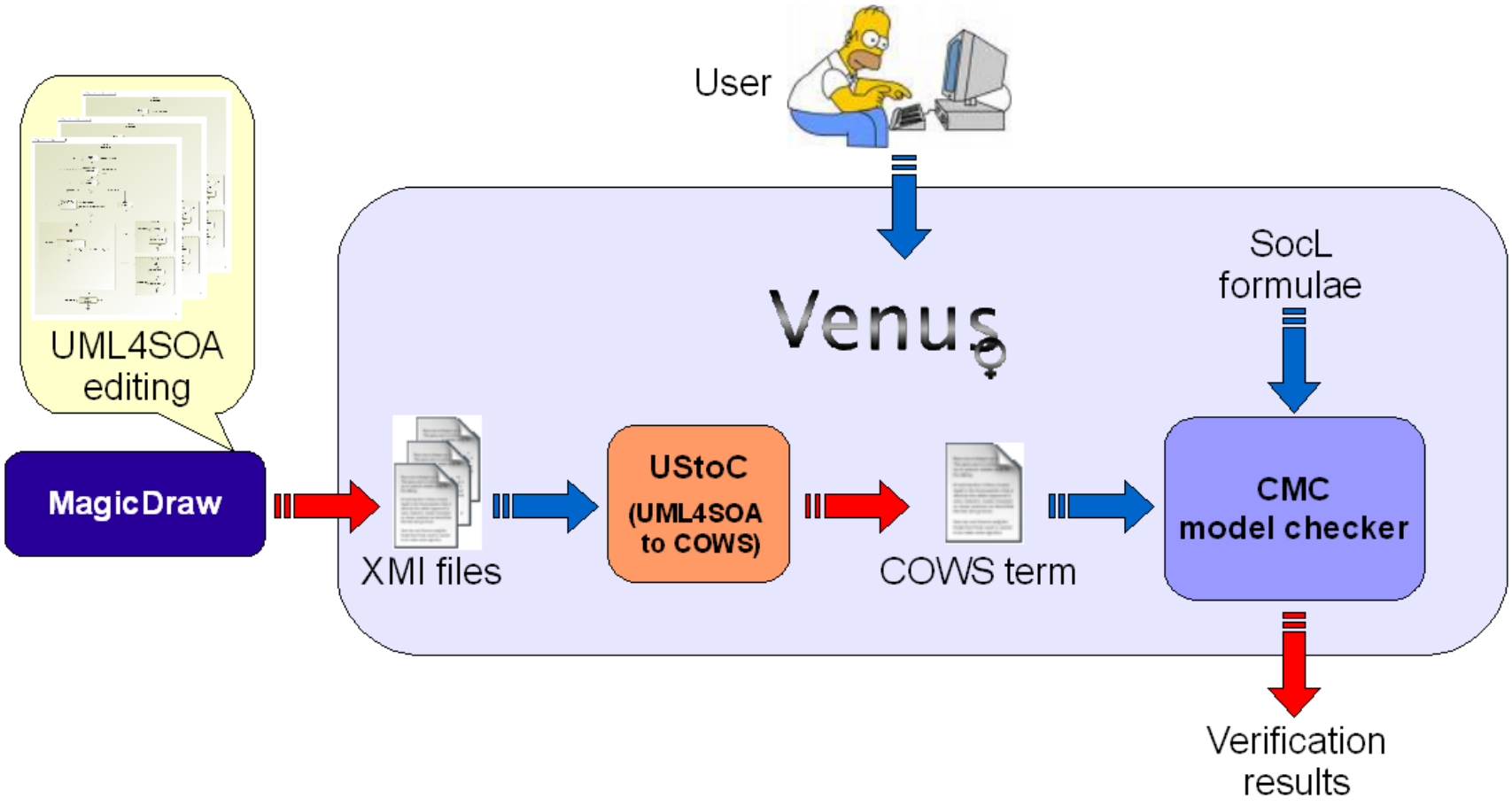
How to reconcile



Our proposal



Our proposal



Tool demonstration . . .

Concluding remarks

- Venus aims at allowing (non-expert) users to verify UML4SOA models of services
- Ongoing and future work:
  - Support the last version of the UML4SOA profile
    - currently, only version 1.2 is supported
  - Refine the CMC feedbacks (e.g. counterexamples)
    - the verification results are already expressed in terms of operations of the UML4SOA specification (by exploiting the CMC abstraction mechanism)
    - however, such output could be still refined to make it more understandable

http://rap.dsi.unifi.it/cows/

Thank you!