

# ON THE SPECIFICATION AND ENFORCEMENT OF PRIVACY-PRESERVING CONTRACTUAL AGREEMENTS

**Gerardo Schneider**



UNIVERSITY OF  
GOTHENBURG

Dept. of Computer Science and Engineering  
Chalmers | Univ. of Gothenburg

[gerardo@cse.gu.se](mailto:gerardo@cse.gu.se)

<http://www.cse.chalmers.se/~gersch/>



CHALMERS



Vetenskapsrådet

Contracts and Computation Workshop  
Göteborg, 2 Nov 2017

**“Consent to give us  
access to your contacts”**

**App: Give me your contact list!**

**Tel: Sure!  
Here it is!**



**Why we do so?**

**We don't read the ToS**

**“All or nothing”:  
Accept it or don't install it**



*It could be nice if...*



**Monitoring and Enforcement**

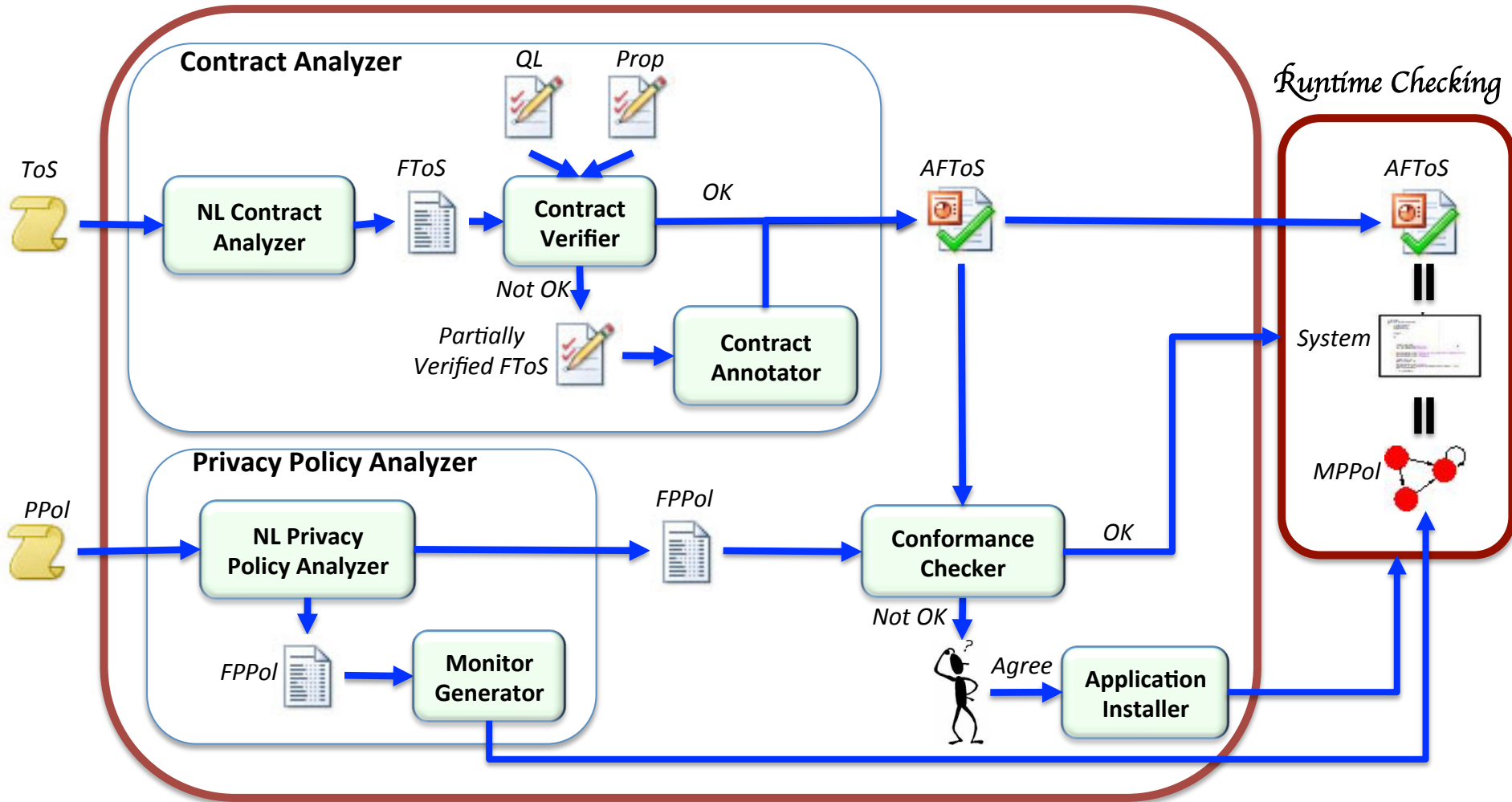


**Conformance**

# **What do we propose?**



# Privacy-Preserving Contractual Agreement Framework

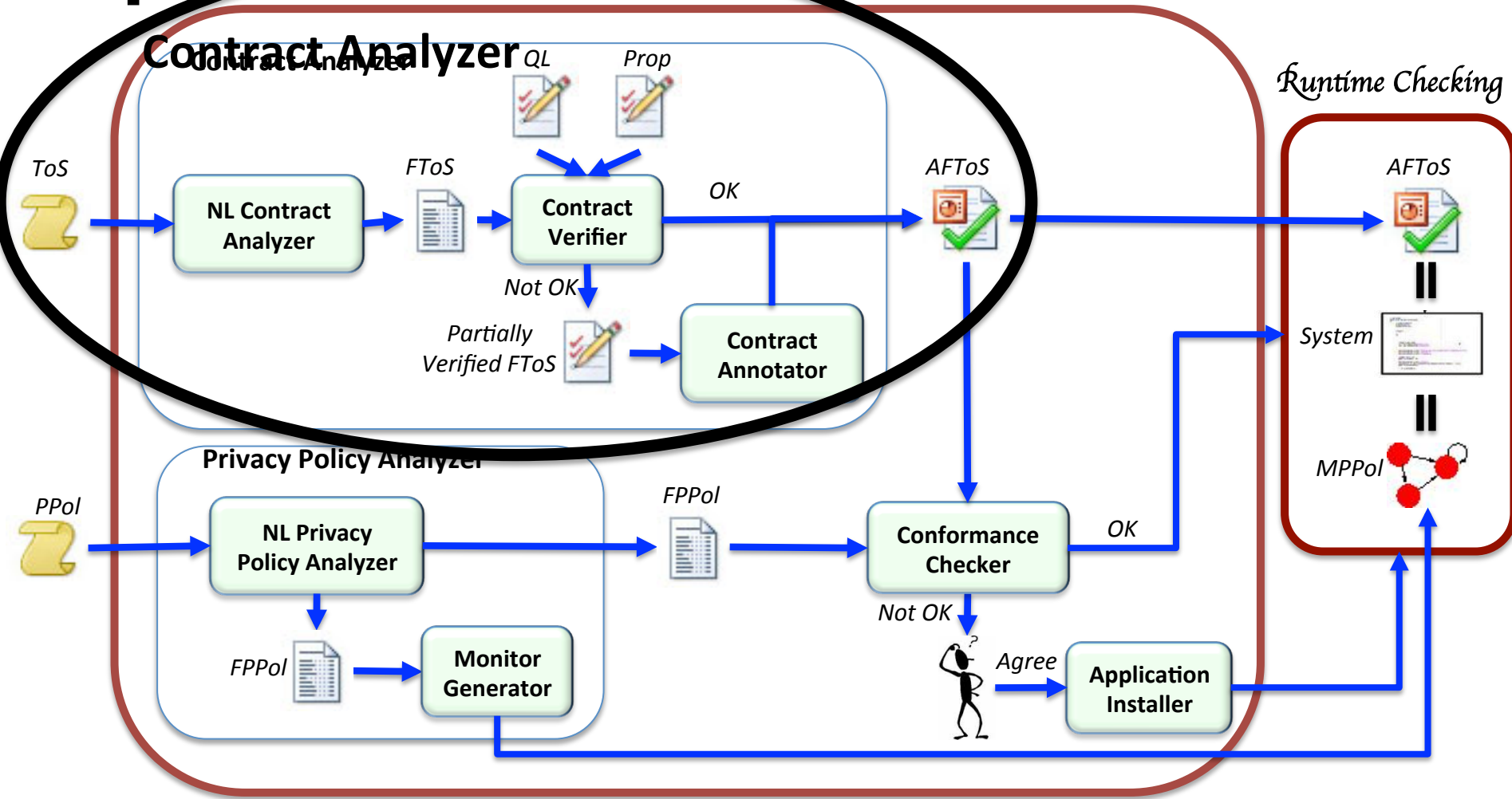


# Privacy-Preserving Contractual Agreement Framework

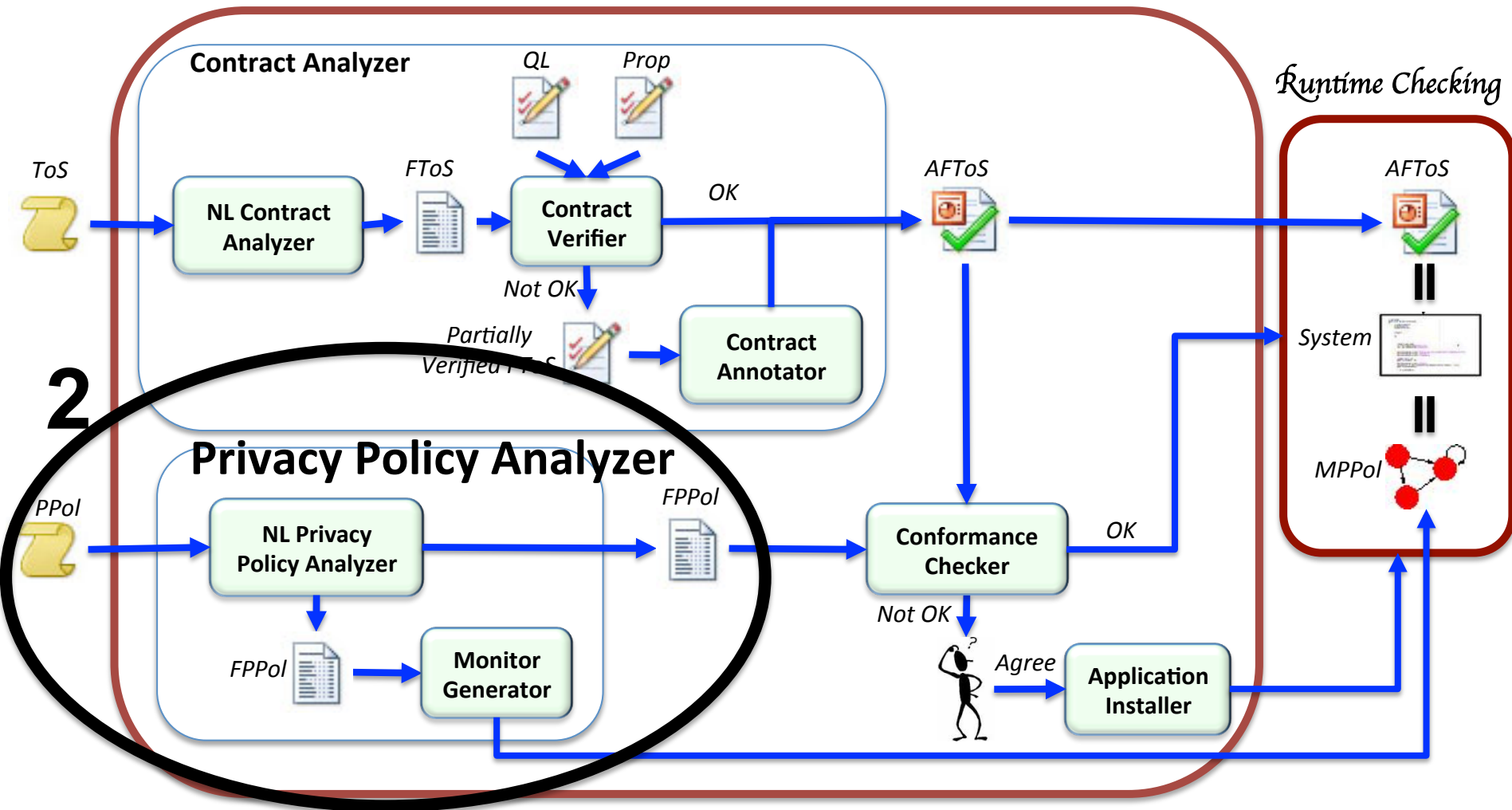
1

## Contract Analyzer

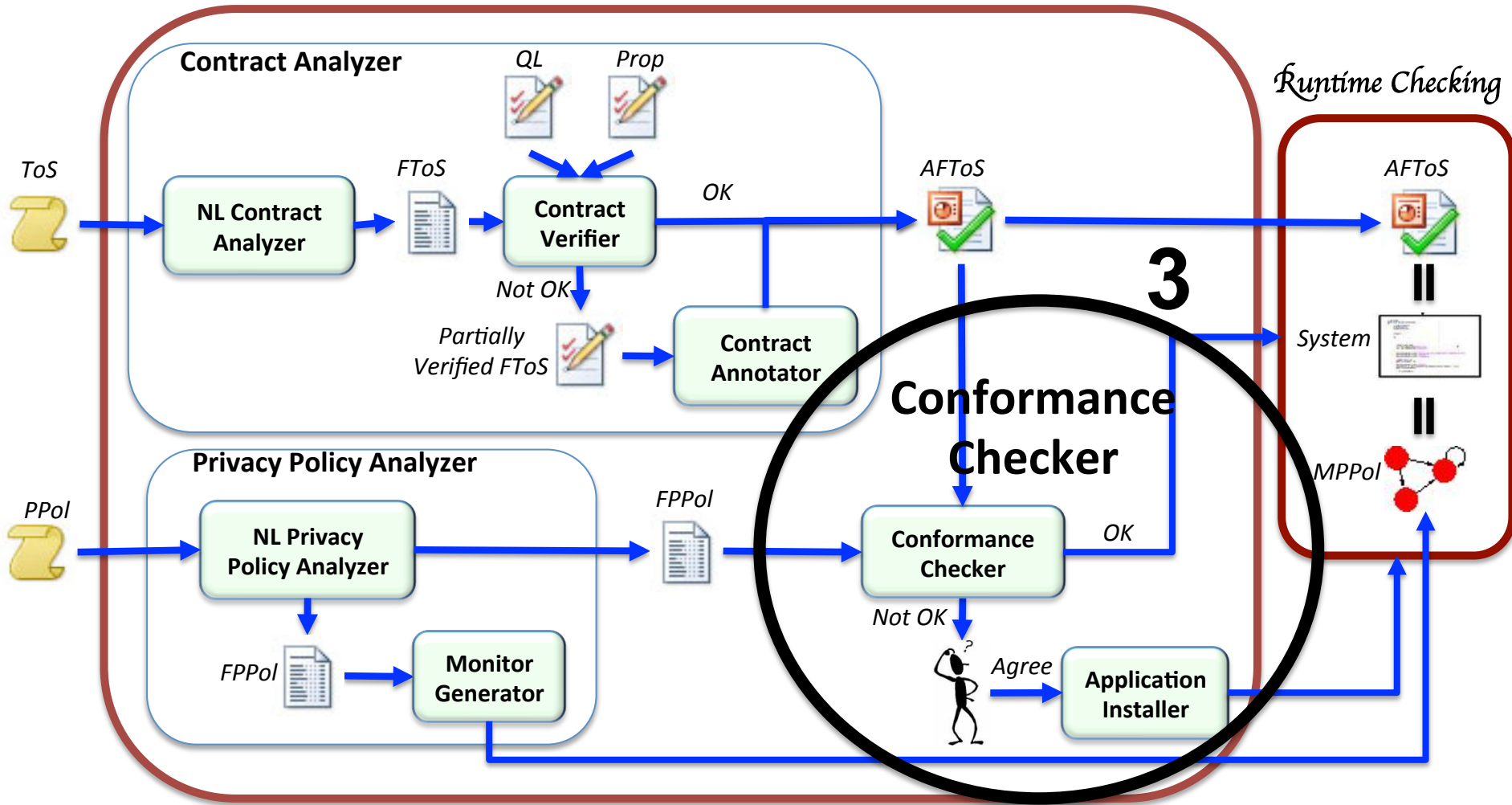
## Runtime Checking



# Privacy-Preserving Contractual Agreement Framework

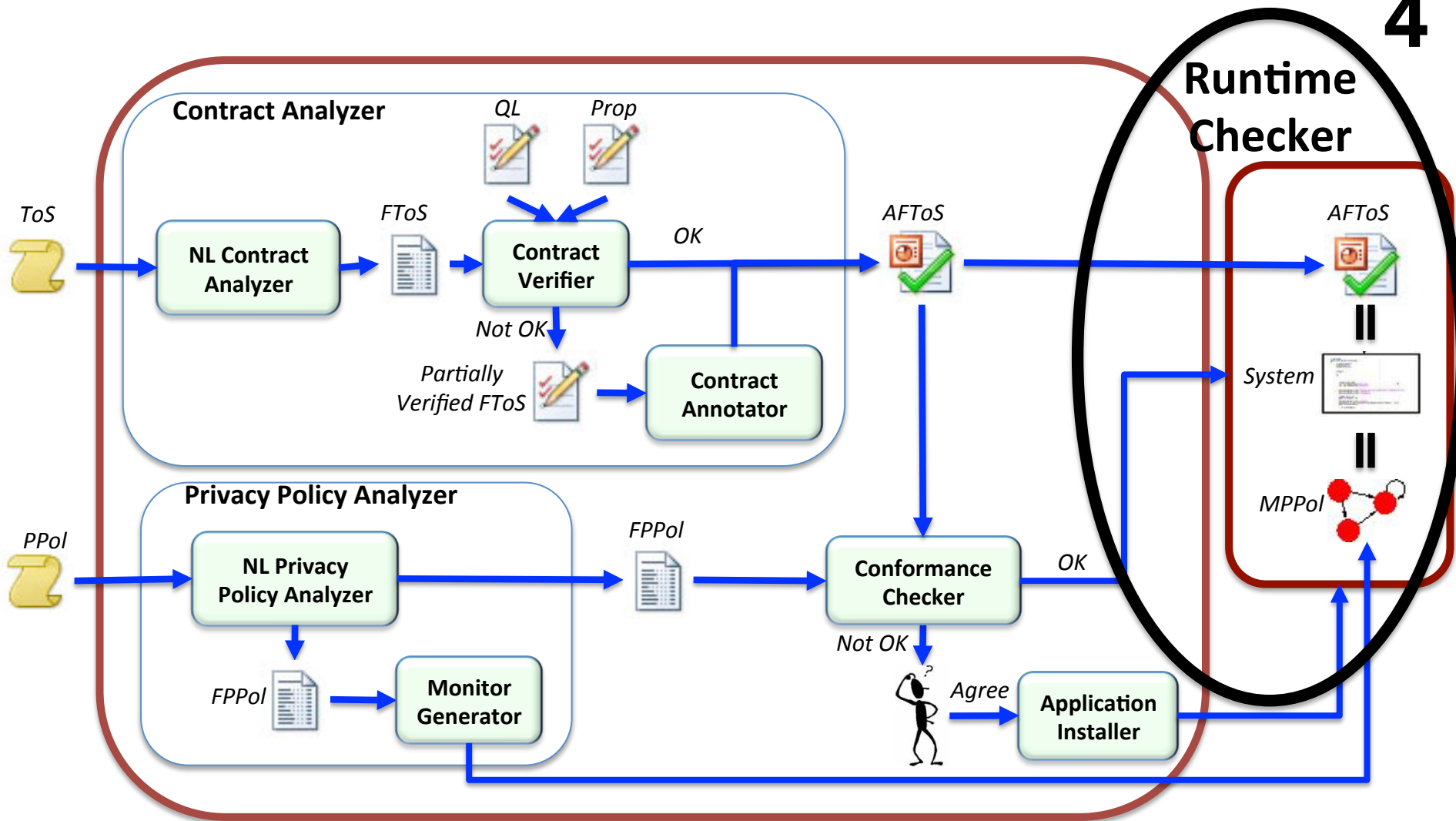


# Privacy-Preserving Contractual Agreement Framework

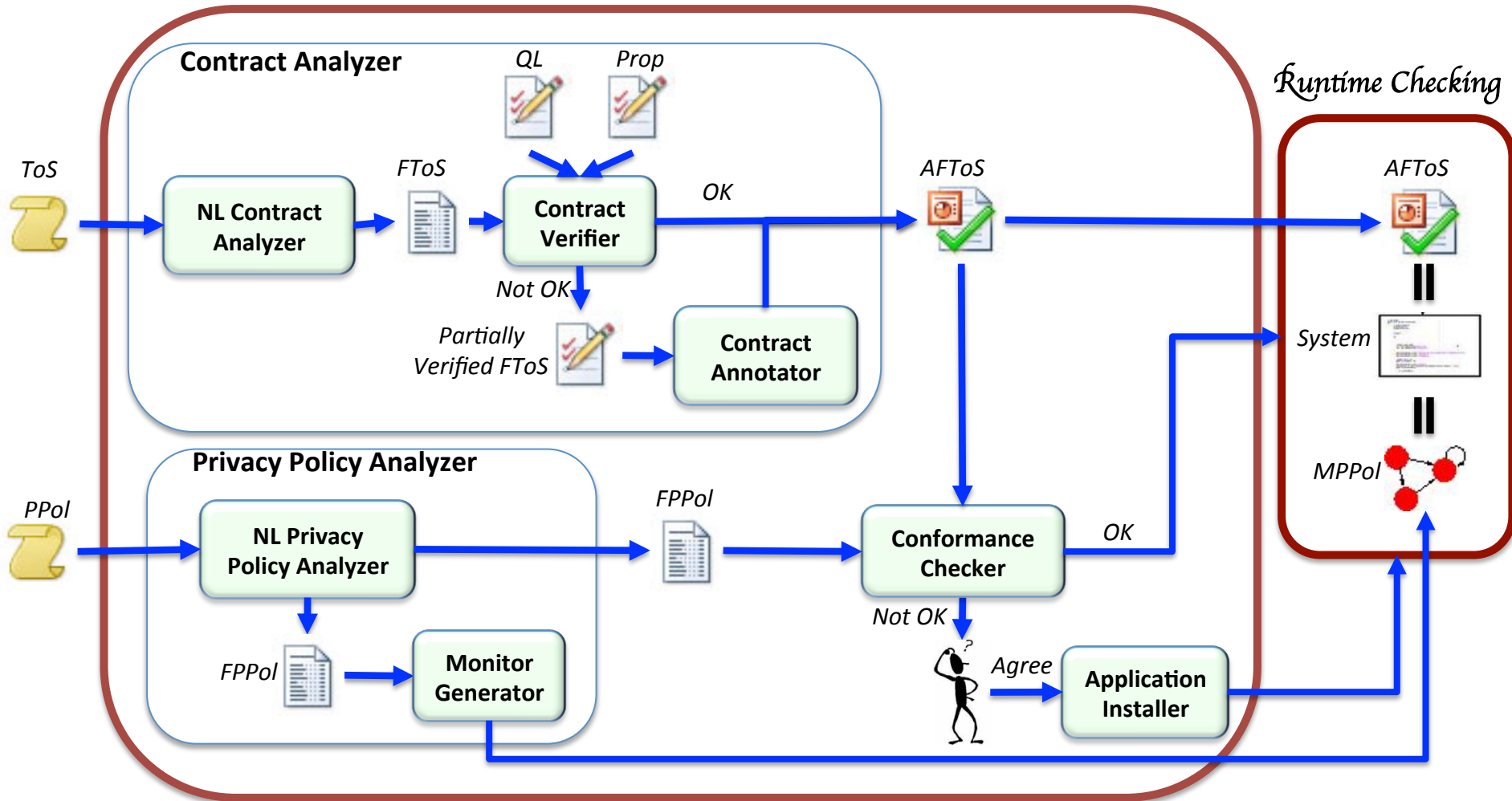


# Privacy-Preserving Contractual Agreement Framework

4

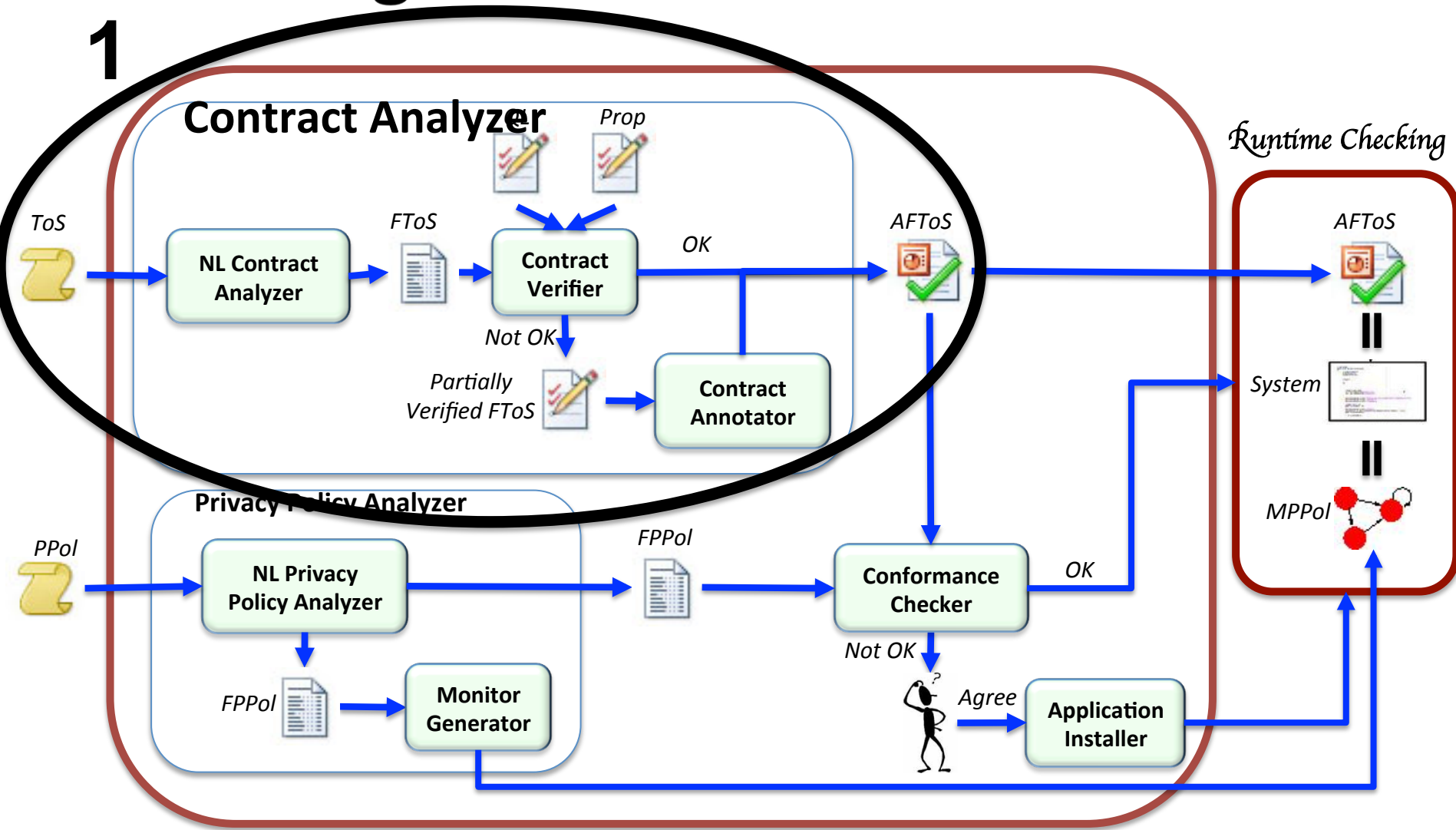


# Privacy-Preserving Contractual Agreement Framework



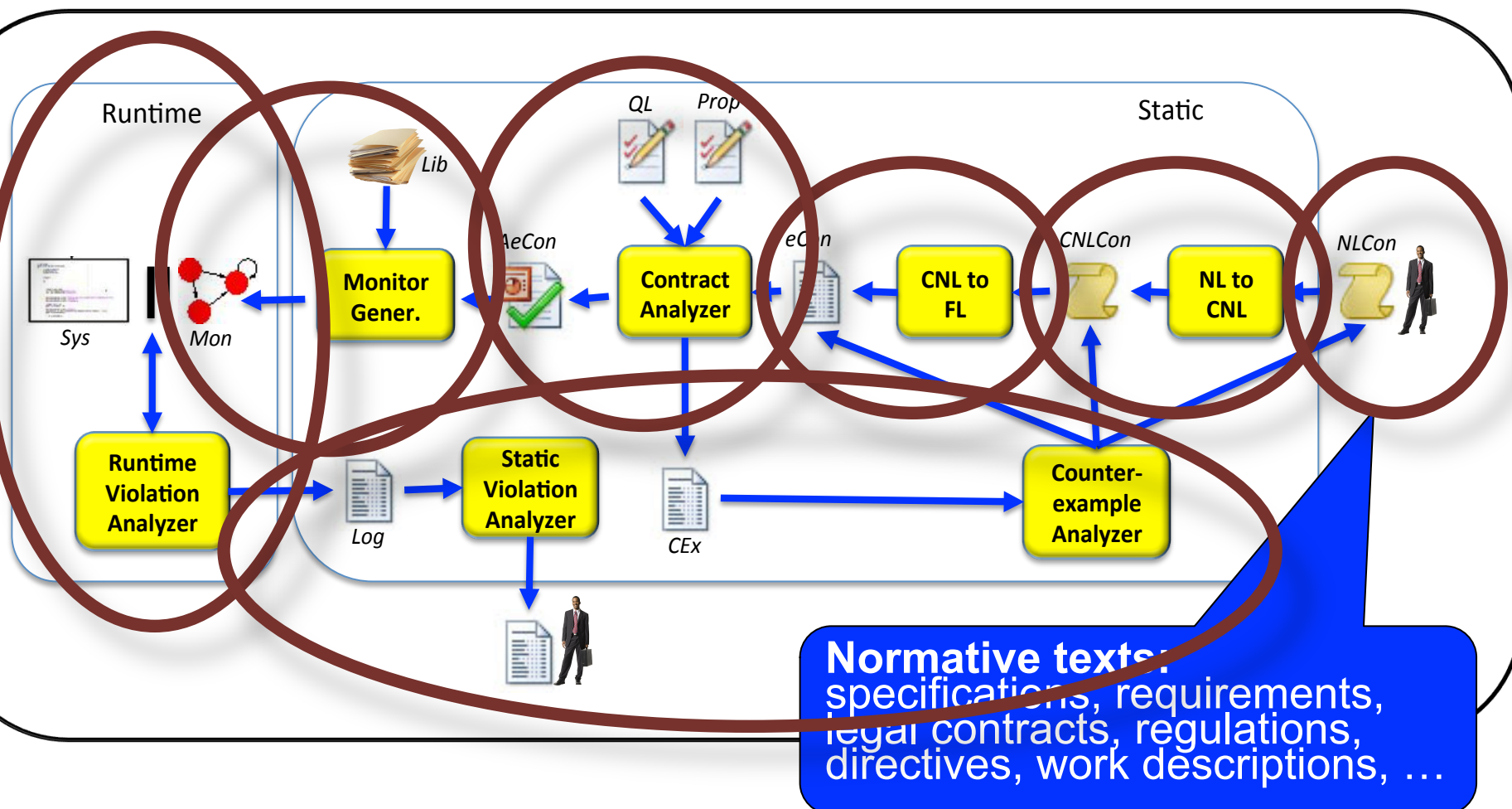
# Privacy-Preserving Contractual Agreement Framework

1





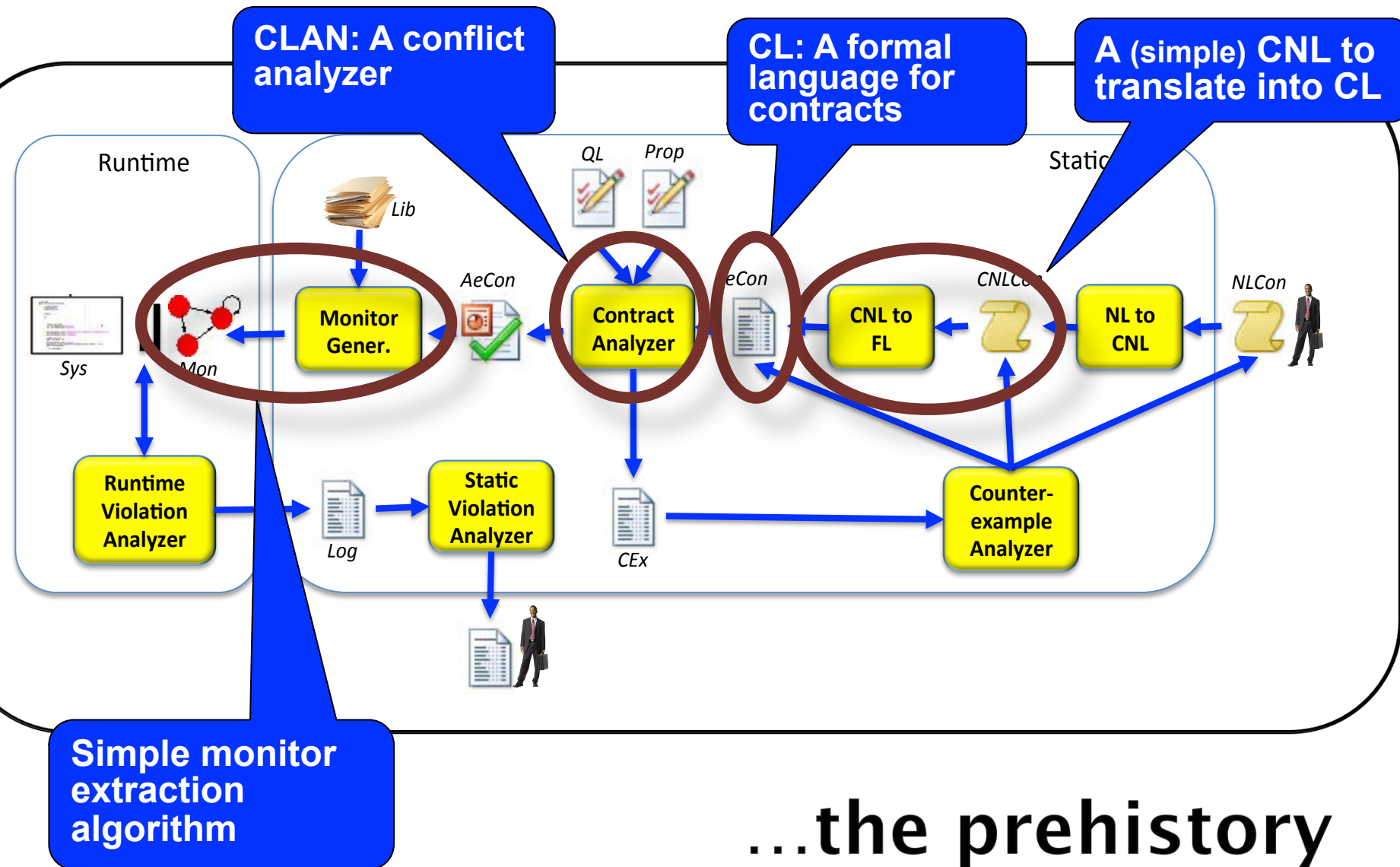
# A high-level scenario on *Contract Analysis*



# ***Contract Analysis***

**What have we done so far?**

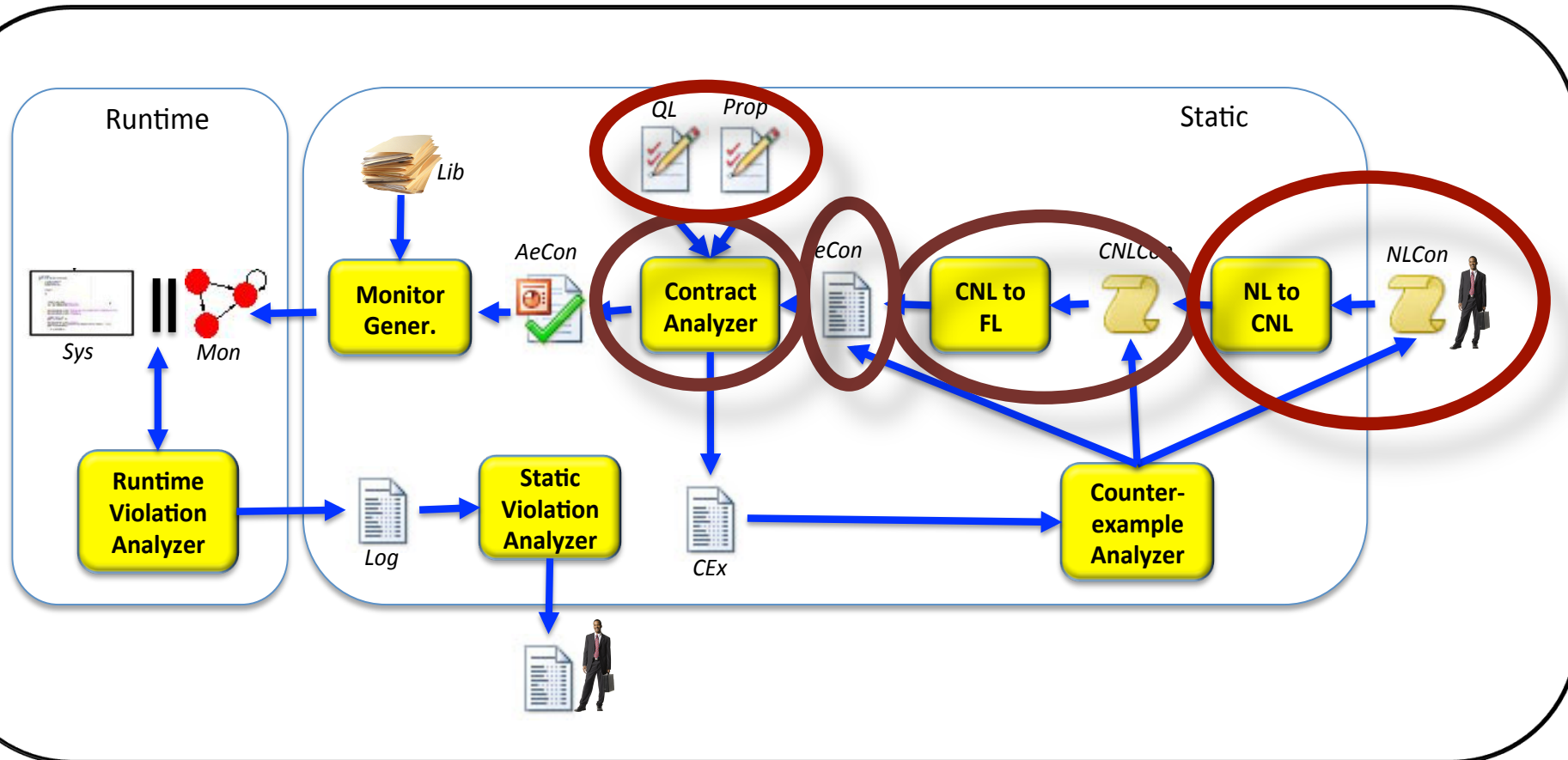
# Small steps towards *Contract Analysis*



...the prehistory

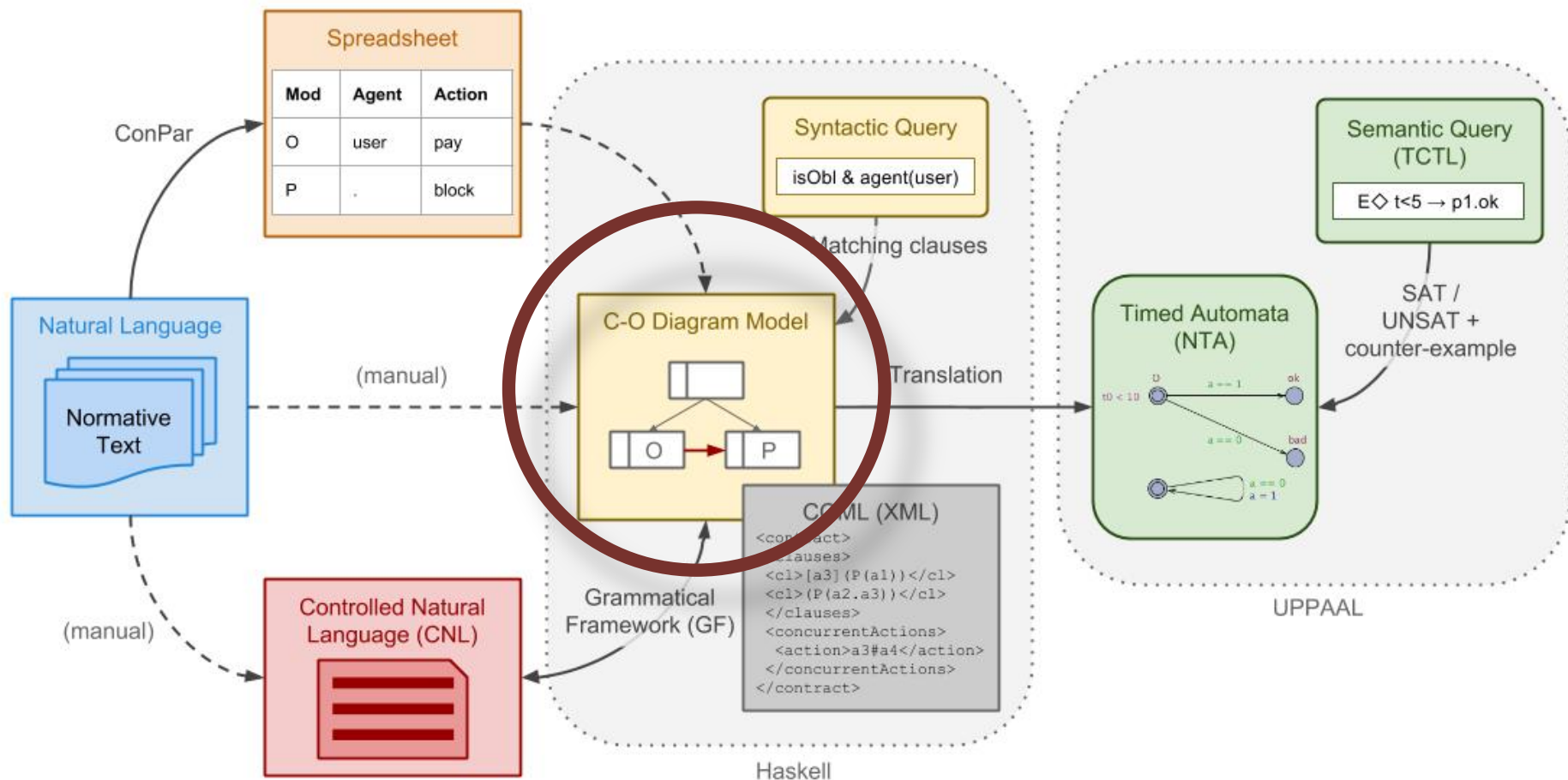
(2006-2011?)

# Small steps towards *Contract Analysis*



...the present  
(since 2012?)

# Small steps towards *Contract Analysis*



\* Proof-of-concept prototype: <http://remu.grammaticalframework.org/contracts/verifier/>

...the present  
(since 2012?)

\* John J. Camilleri *et al* (since 2014...)

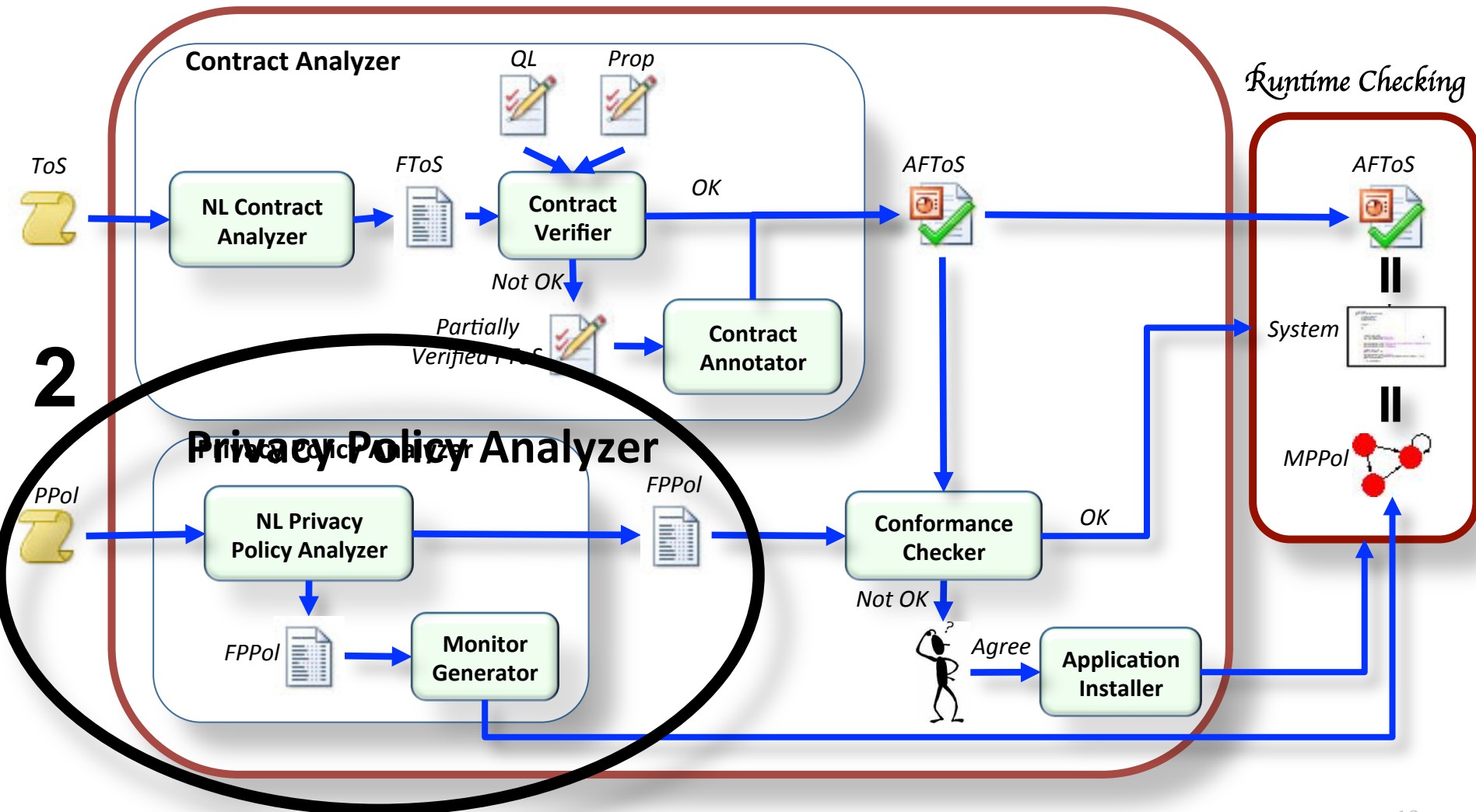
\* Enrique Martínez *et al* (2012-2013)

Gerardo Schneider

# (A bit more on contracts...)

- Contract Automata
  - With G. Pace and F. Schapachnik
- (Smart Contracts...)

# Privacy-Preserving Contractual Agreement Framework



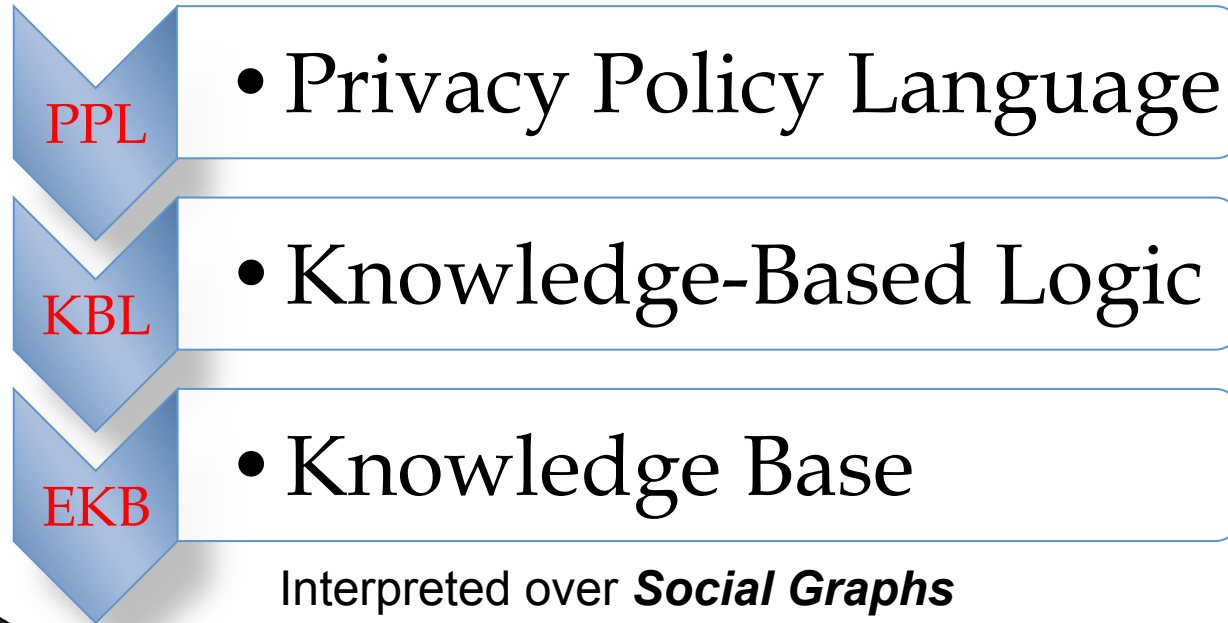


# ***Privacy Policies***

**What have we done so far?**

# Very small **steps towards *Privacy Policies***

## PPF: Privacy Policy Framework



For Social Networks

"Evolving" policies:

- Automata
- Real-Time

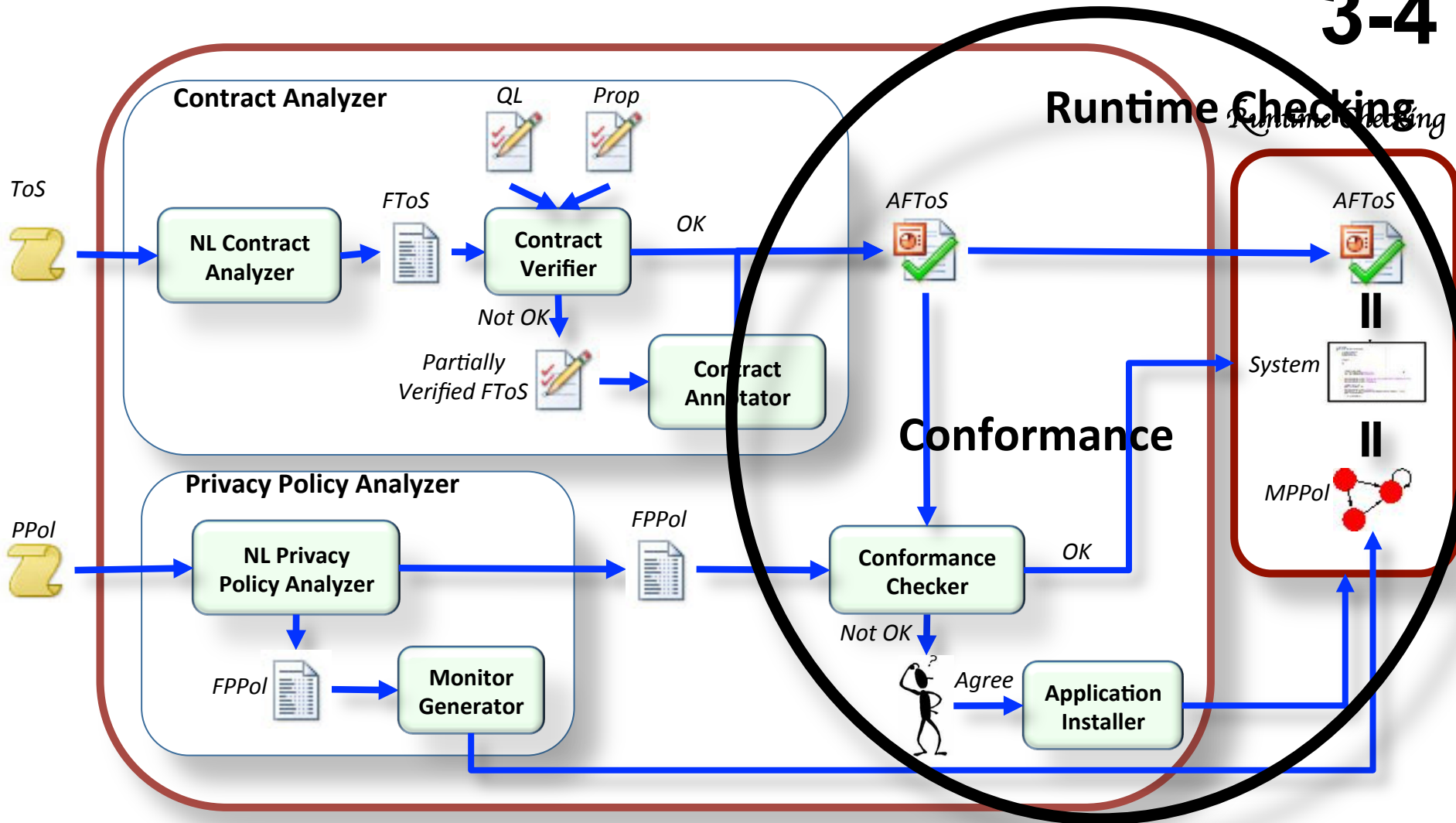
Need to be adapted as a stand-alone framework  
(Syntax OK, but semantics...)

# (A bit more on privacy... GDPR)

- Privacy-by-Design
  - With T. Antignac and R. Scandariato
- Personalized differential privacy
  - With H. Ebadi and D. Sands
- Language-based approach to data minimization
  - With T. Antignac and D. Sands
- Runtime monitoring of hyper-properties
  - With S. Pinisetty and D. Sands
- Privacy leaks on browser extensions
  - With P. Picazo-Sánchez and J. Tapiador
- ...

# Privacy-Preserving Contractual Agreement Framework

3-4



# ***Conformance Checking***

## ***Runtime Checking***

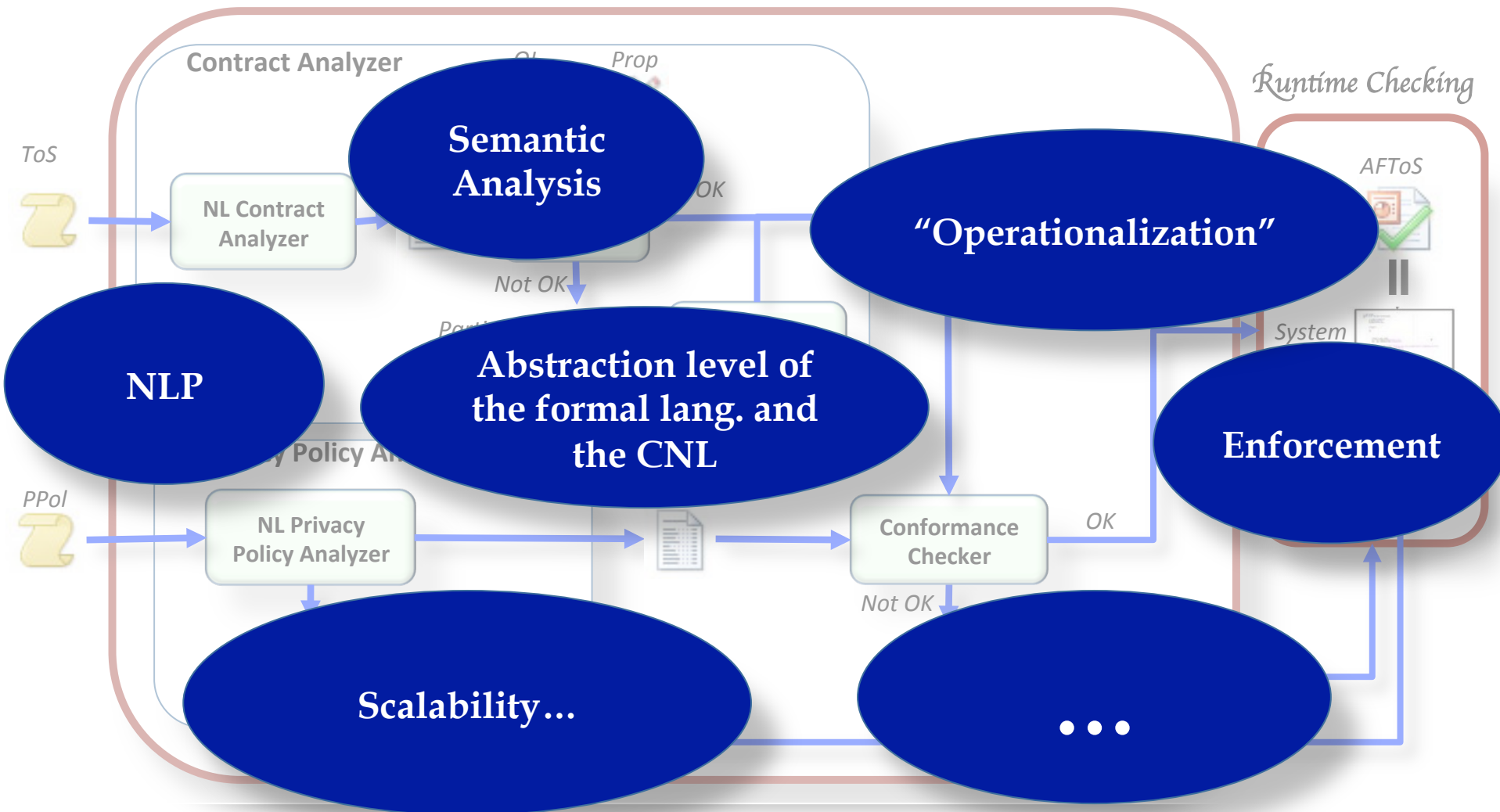
**What have we done so far?**

**Not much...**

# (A bit more on runtime monitoring, verification and enforcement...)

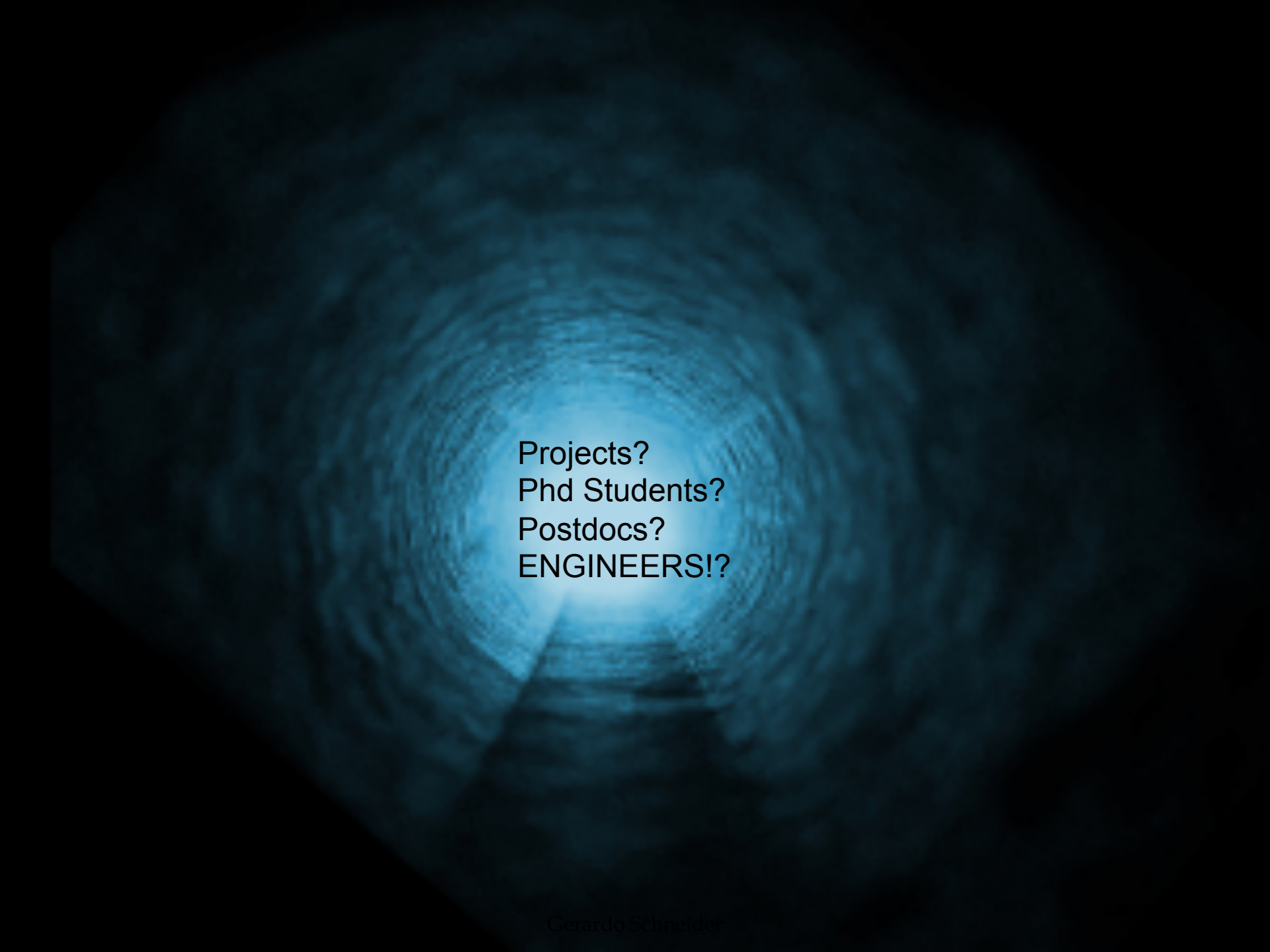
- LARVA (Automata-based approach)
  - With C. Colombo and G. Pace
- Combining static and runtime verification
  - With W. Ahrendt, M. Cimento, and G. Pace
- Different theoretical results and applications of runtime verification and enforcement
  - With S. Pinisetty
- Migrating monitors and IoT
  - With P. Picazo-Sánchez and G. Pace
- ...

# A lot of challenges!



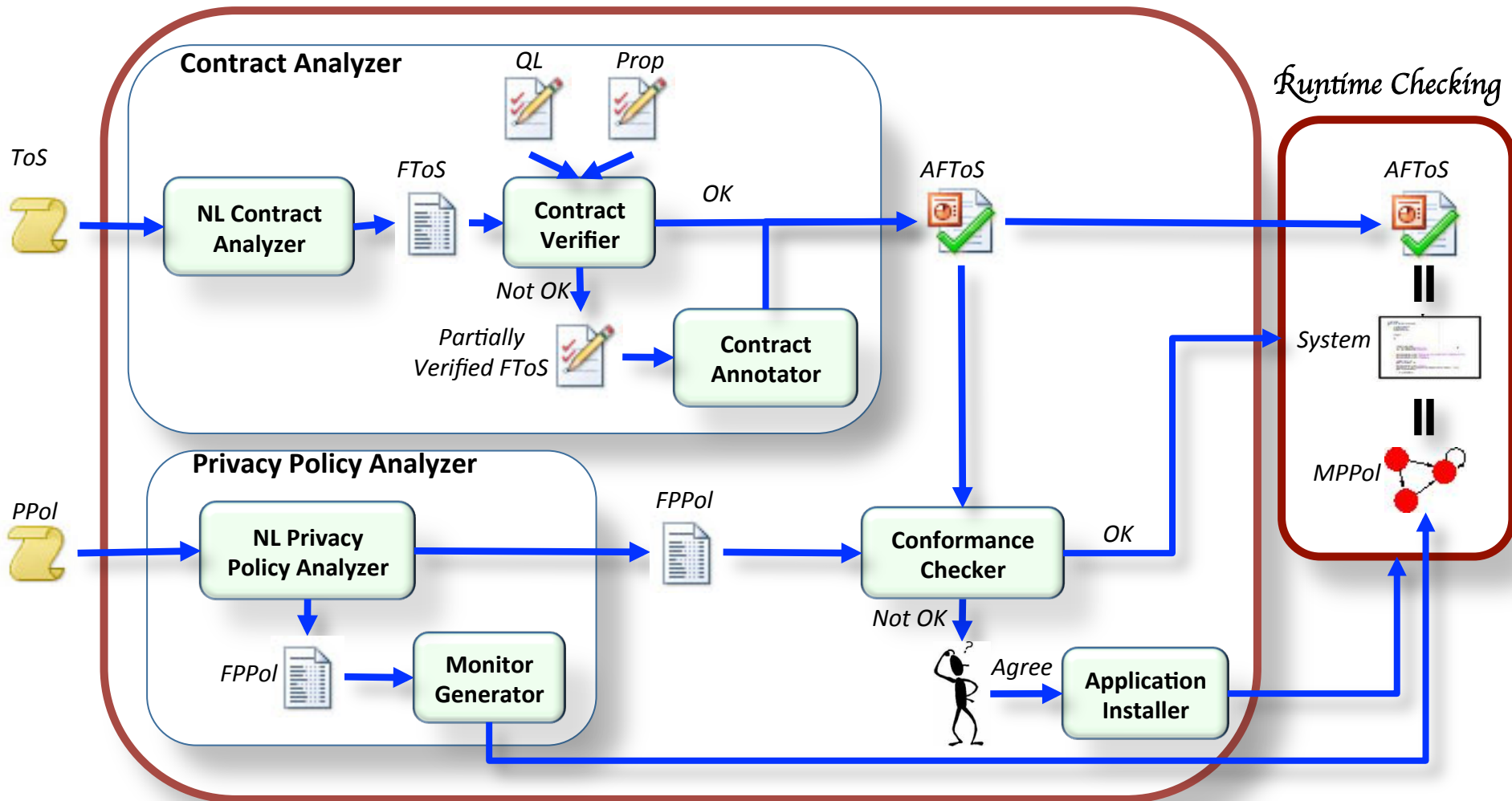






Projects?  
Phd Students?  
Postdocs?  
**ENGINEERS!?**

# Still a lot to be done...



PRESS RELEASE 2016-10-10



## ***The Prize in Economic Sciences 2016***

The Royal Swedish Academy of Sciences has decided to award the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred **Nobel** 2016 to

***Oliver Hart***, Harvard University, Cambridge, MA, USA, and  
***Bengt Holmström***, Massachusetts Institute of Technology,  
Cambridge, MA, USA

“for their contributions to **contract theory**”