

ON THE SPECIFICATION AND ENFORCEMENT OF PRIVACY-PRESERVING CONTRACTUAL AGREEMENTS

(or... a summary of some of my work in the area)

Gerardo Schneider



UNIVERSITY OF
GOTHENBURG

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

gerardo@cse.gu.se

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



CHALMERS



Vetenskapsrådet

ARVI COST action: Workshop on Contracts
Prague, Czech Republic
March 17, 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...



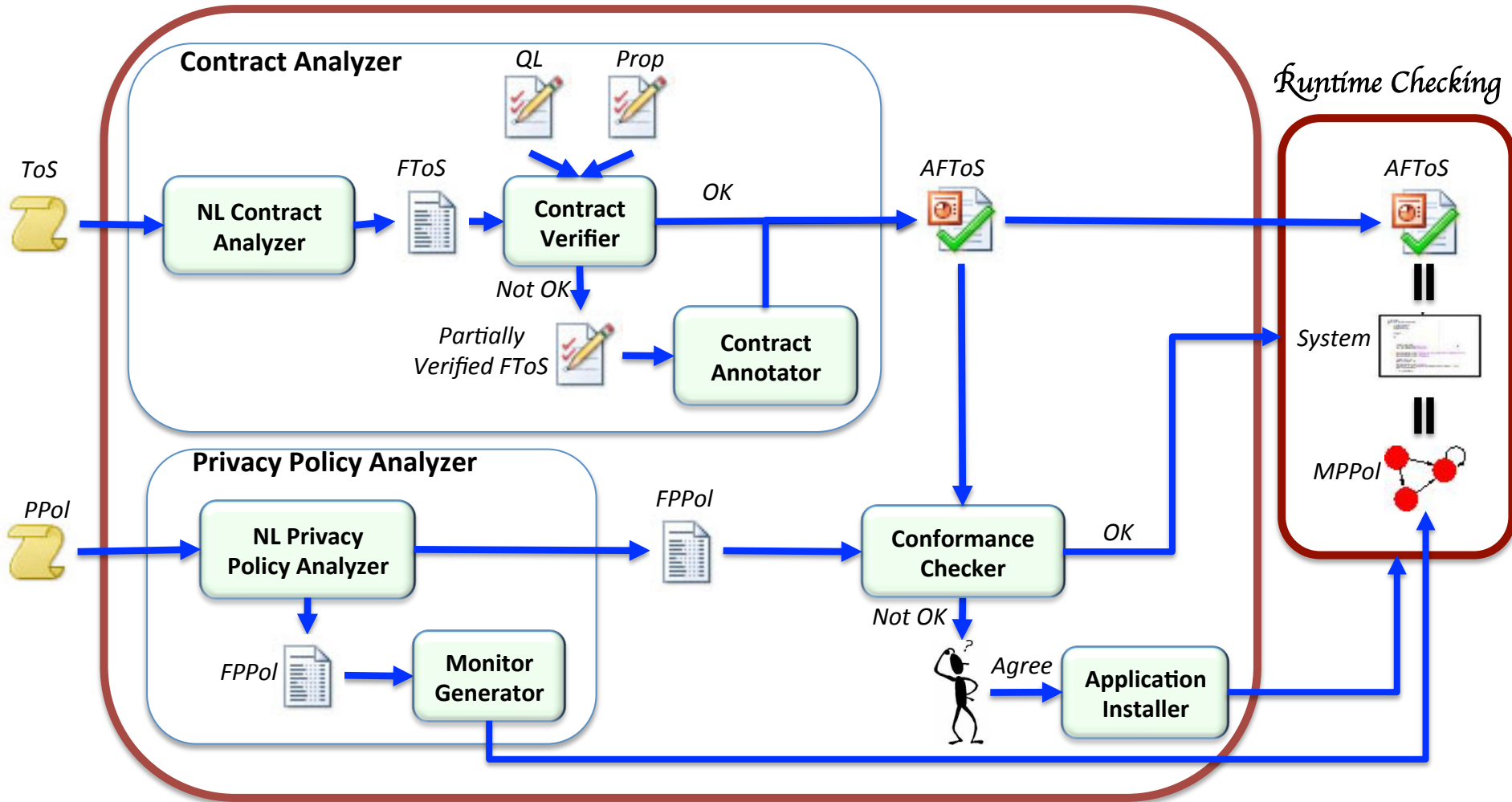
Monitoring and Enforcement



Conformance

What do we propose?

Privacy-Preserving Contractual Agreement Framework

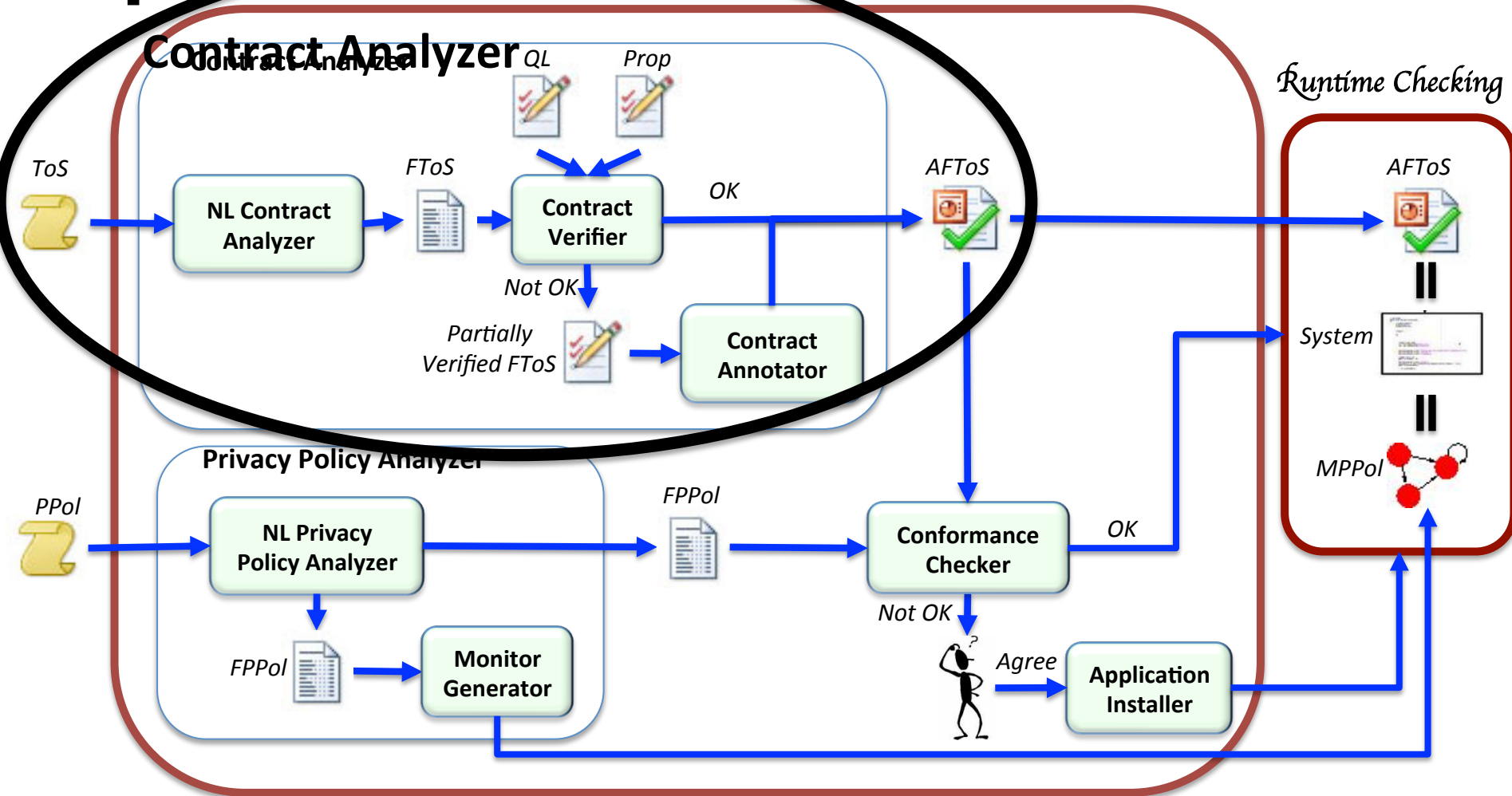


Privacy-Preserving Contractual Agreement Framework

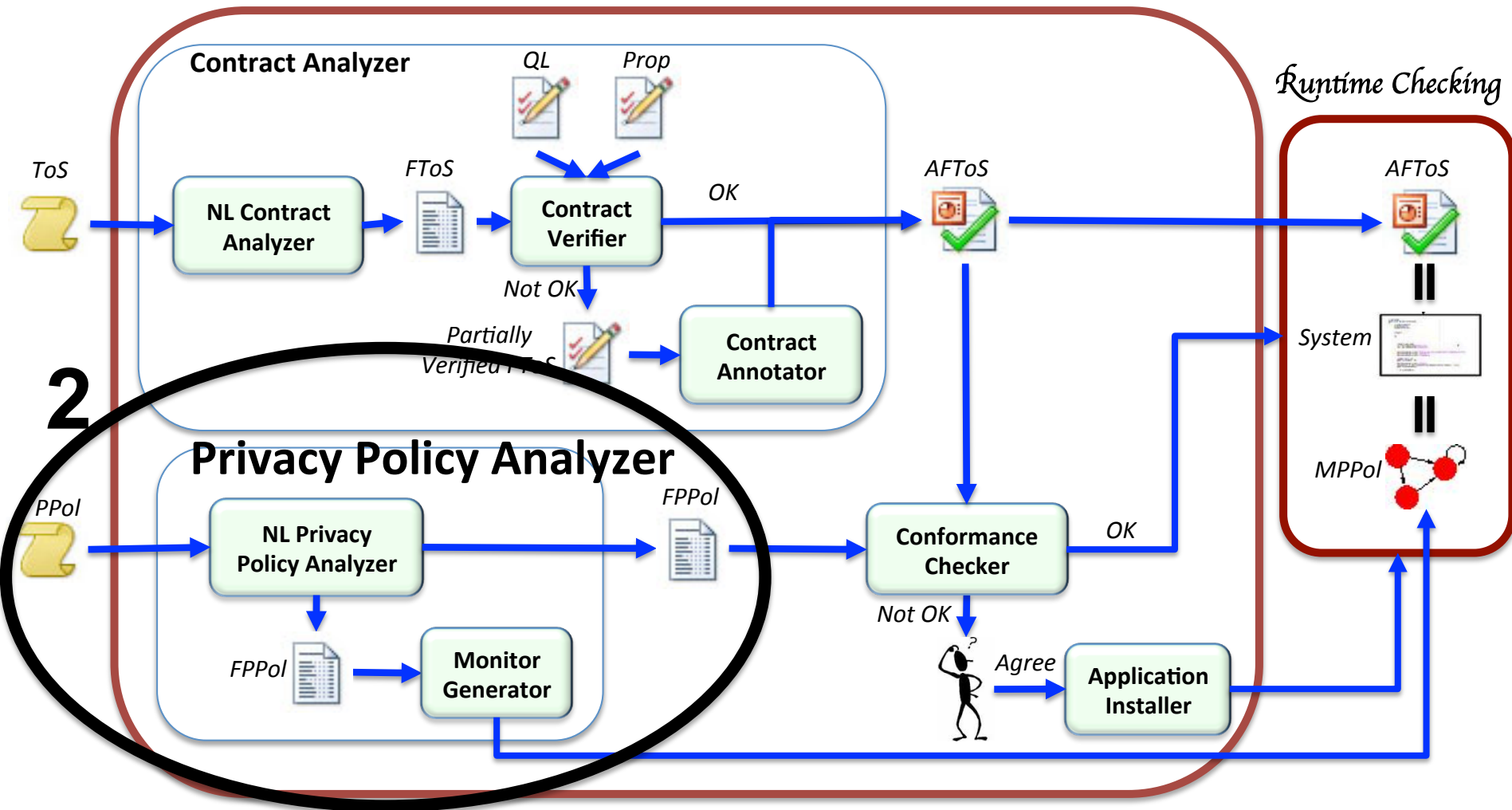
1

Contract Analyzer

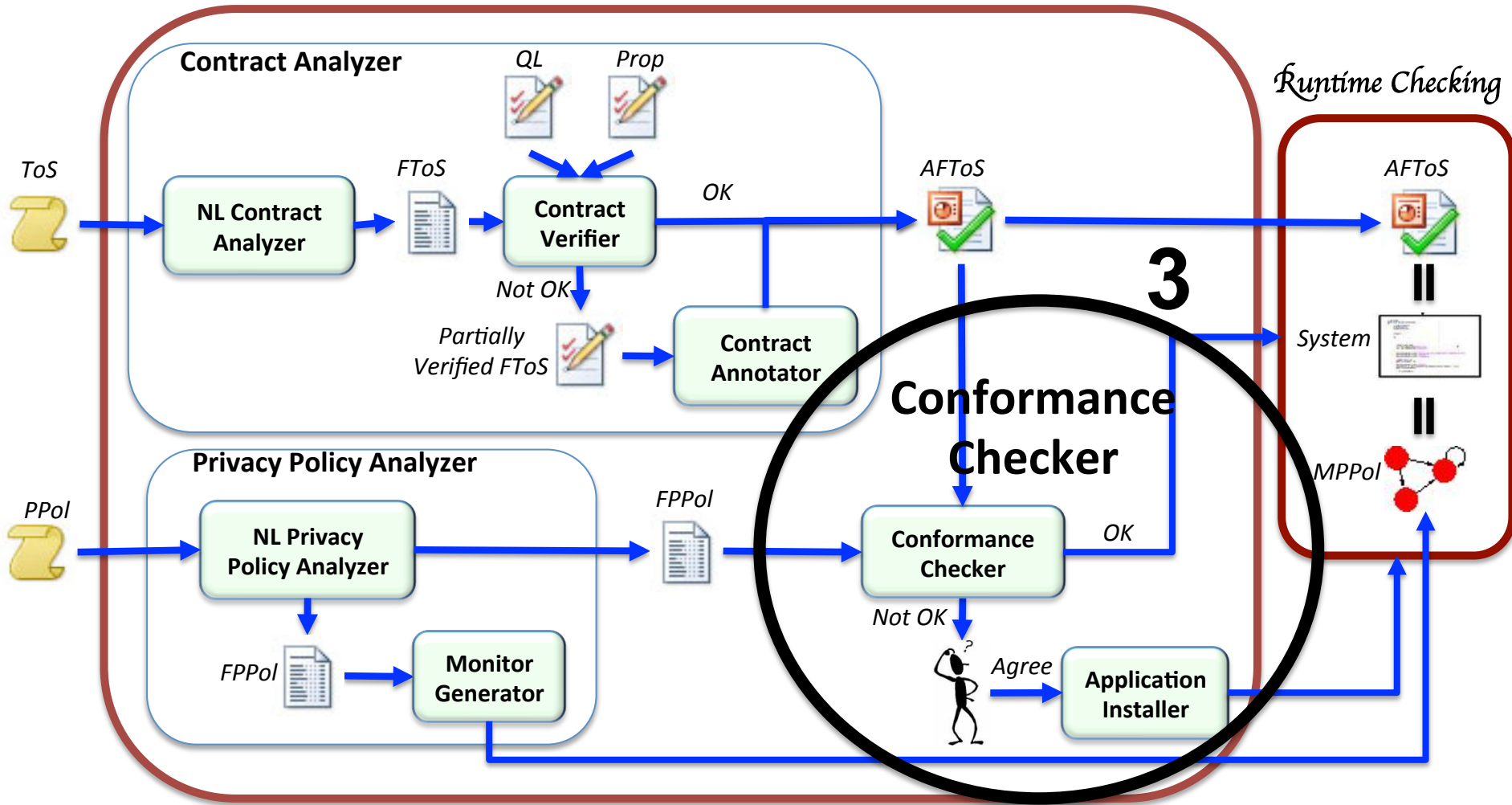
Runtime Checking



Privacy-Preserving Contractual Agreement Framework

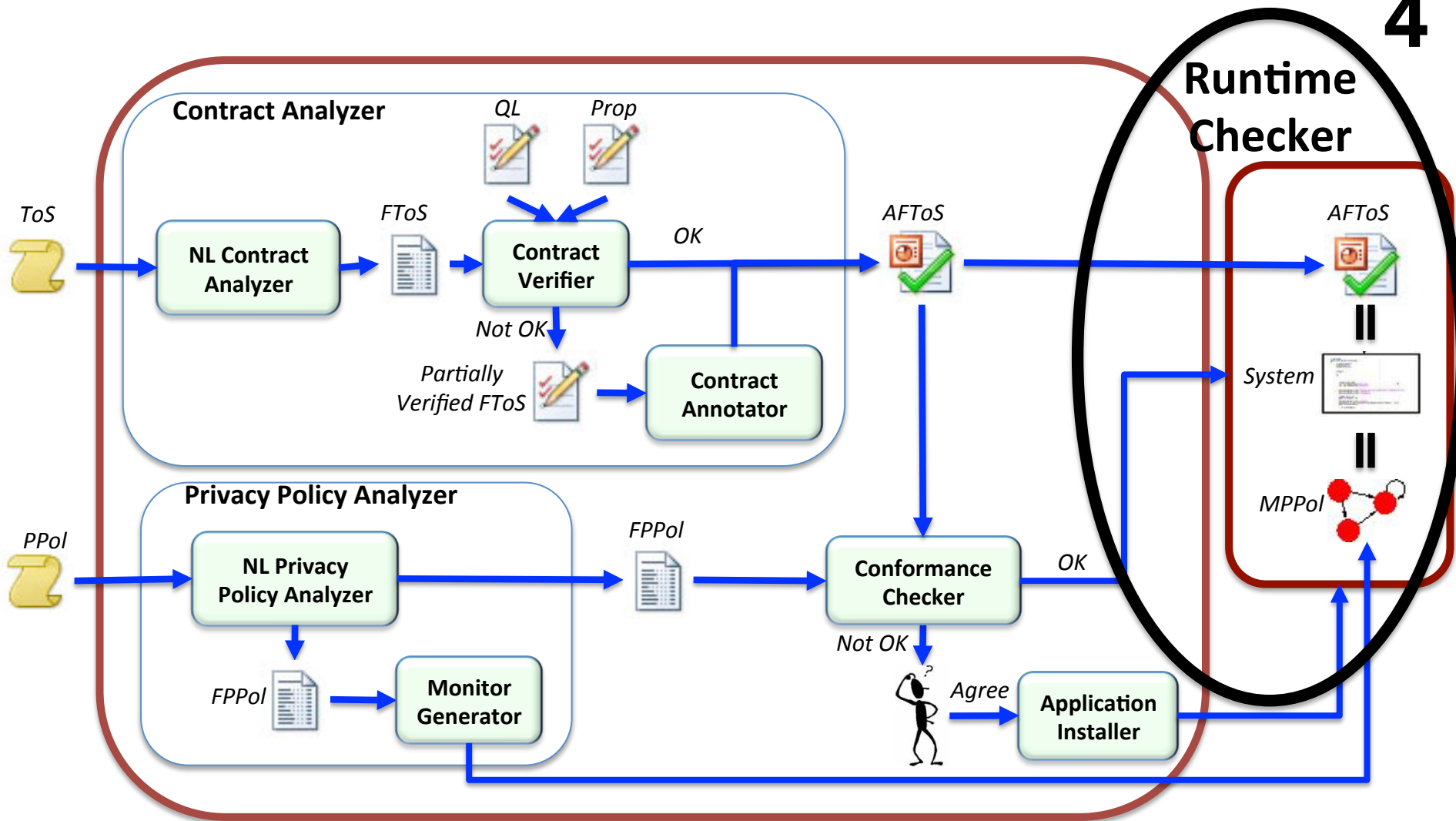


Privacy-Preserving Contractual Agreement Framework

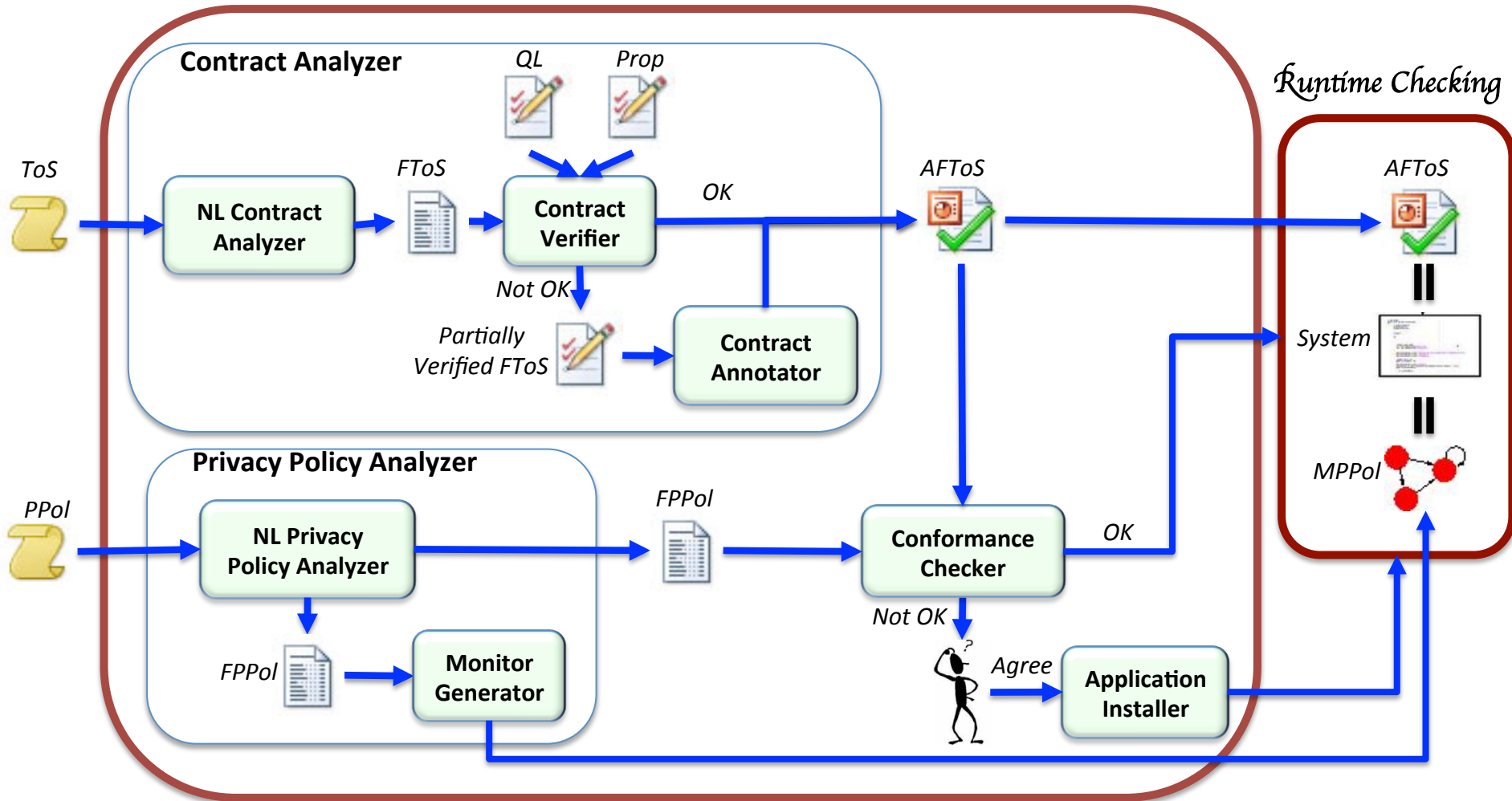


Privacy-Preserving Contractual Agreement Framework

4

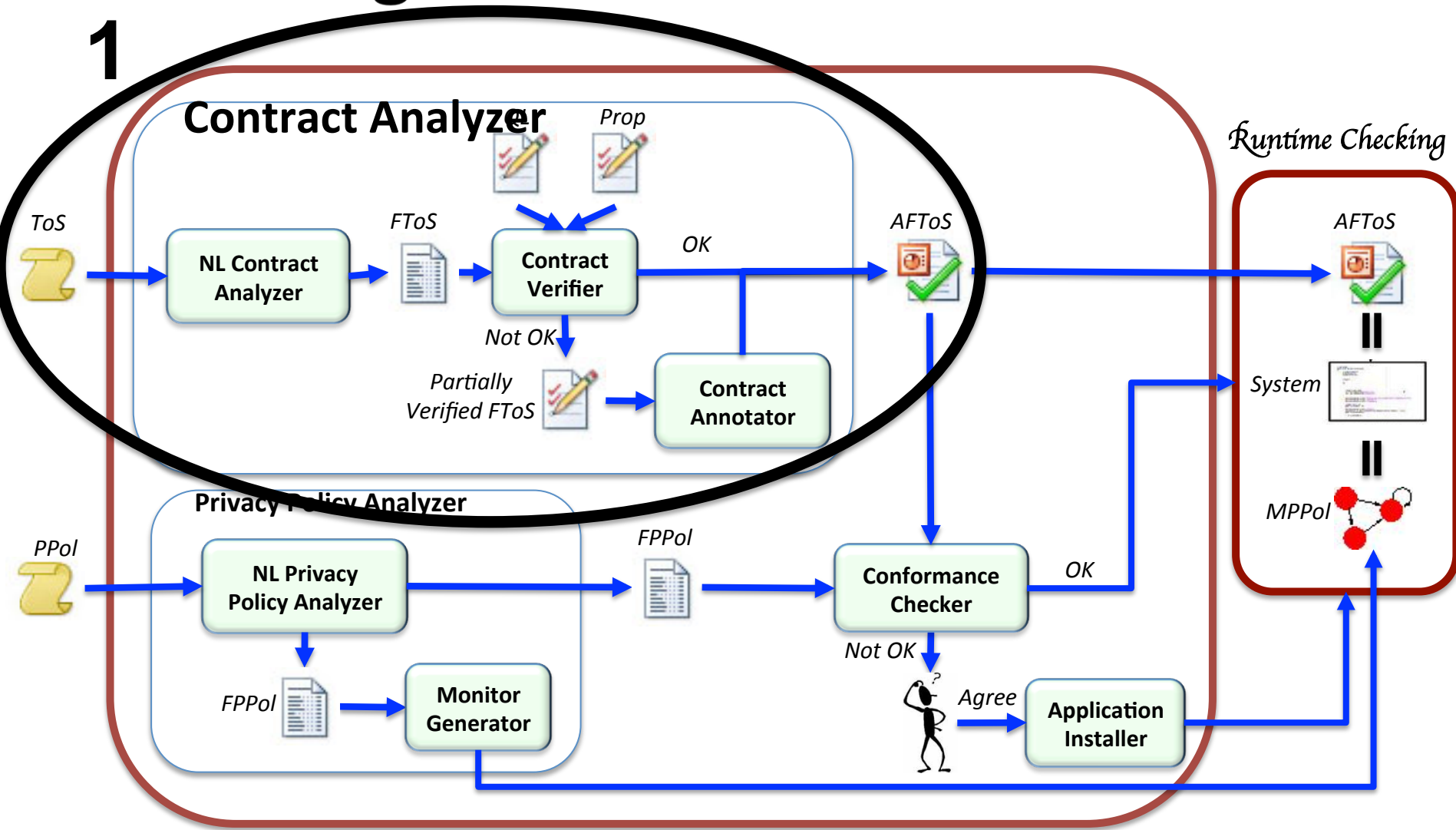


Privacy-Preserving Contractual Agreement Framework

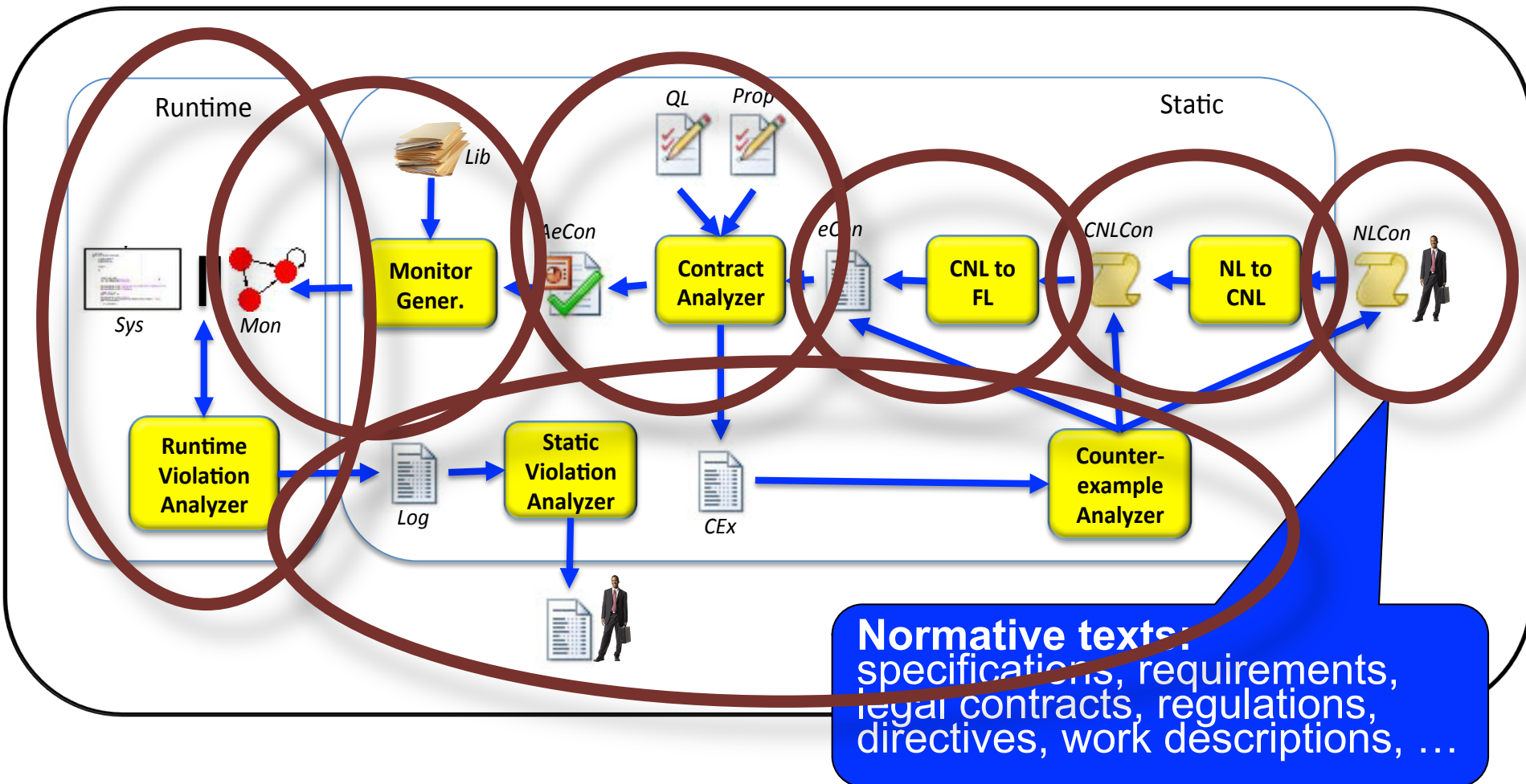


Privacy-Preserving Contractual Agreement Framework

1



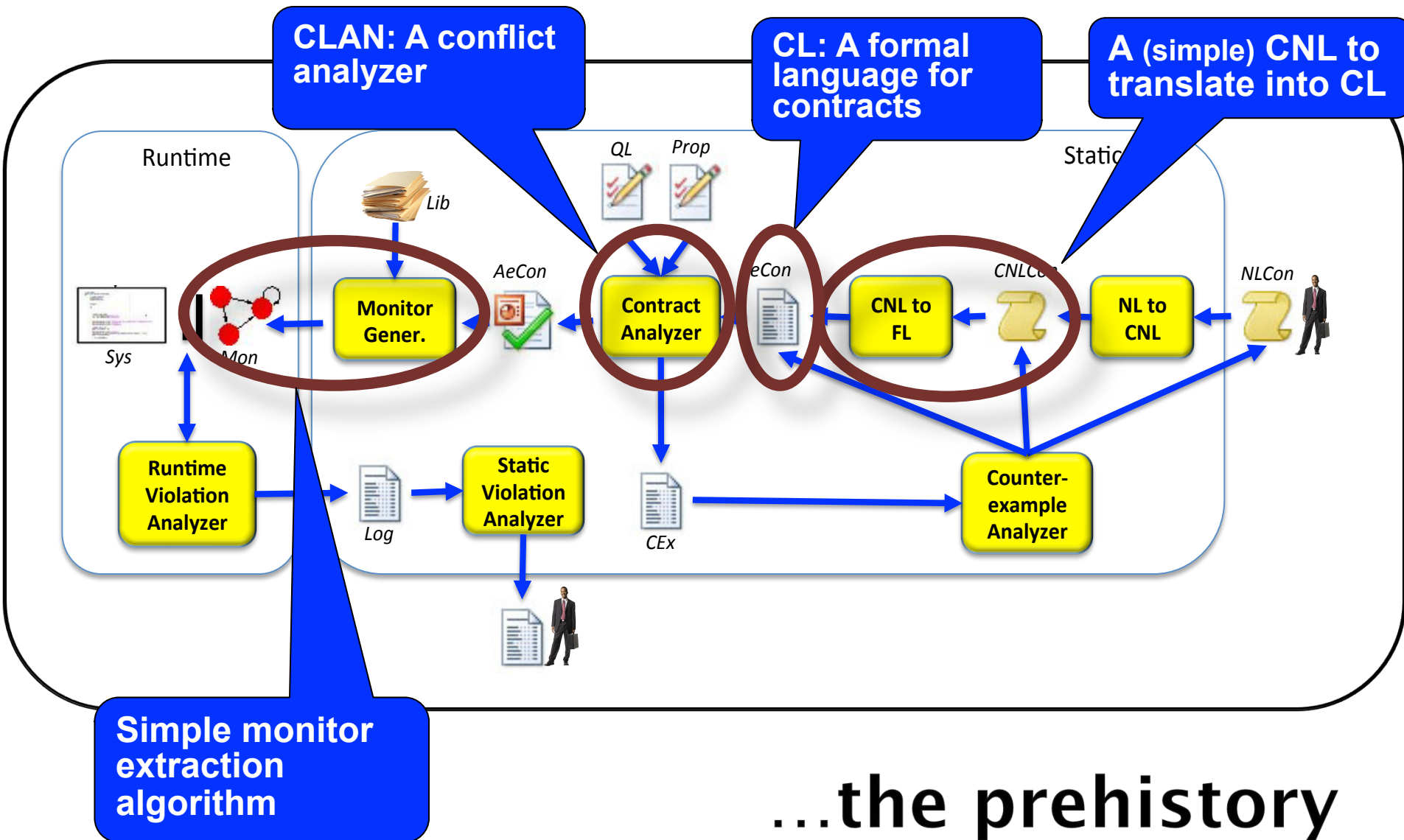
A high-level scenario on *Contract Analysis*



Contract Analysis

What have we done so far?

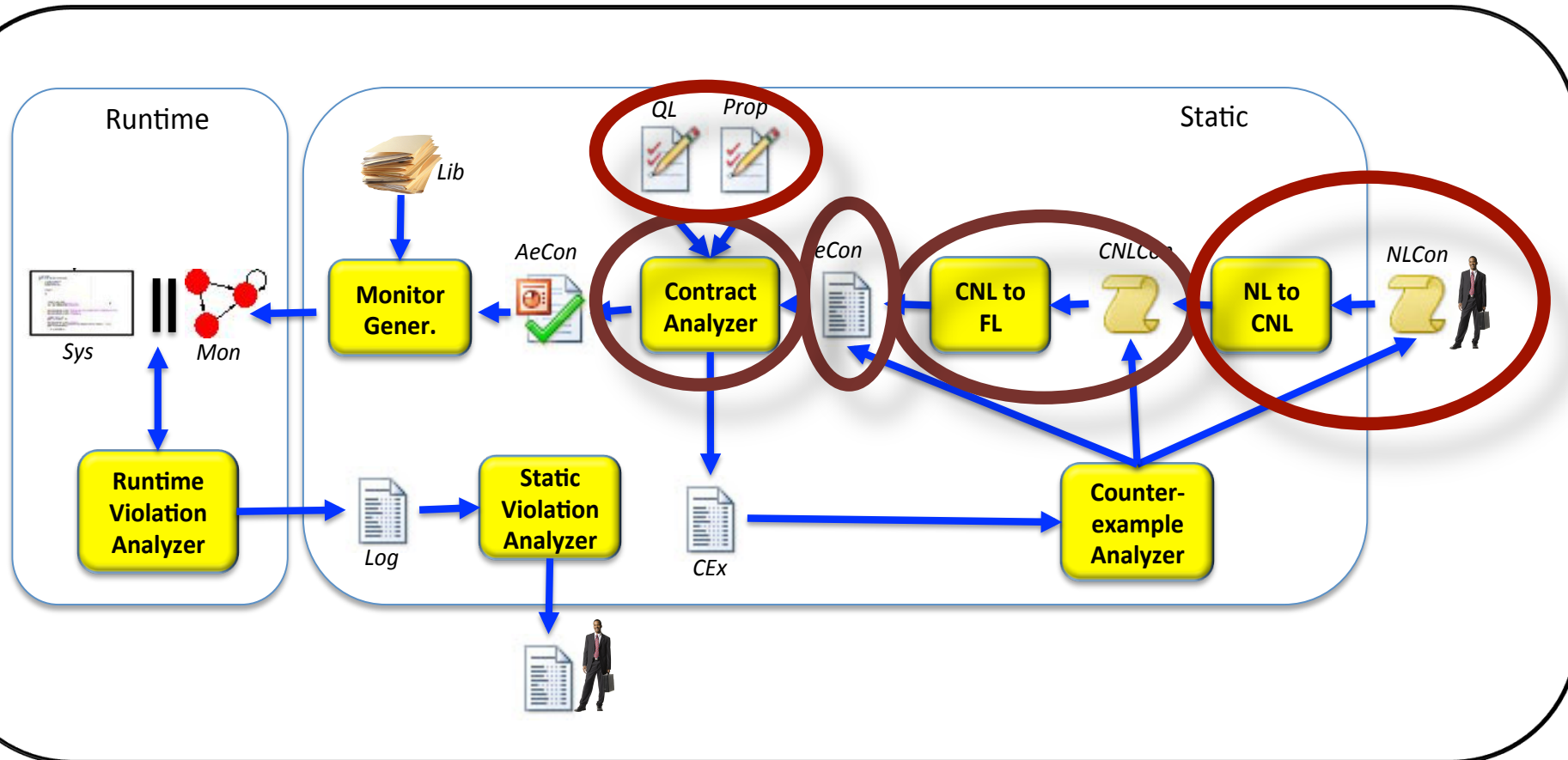
Small steps towards *Contract Analysis*



...the prehistory

(2006-2011?)

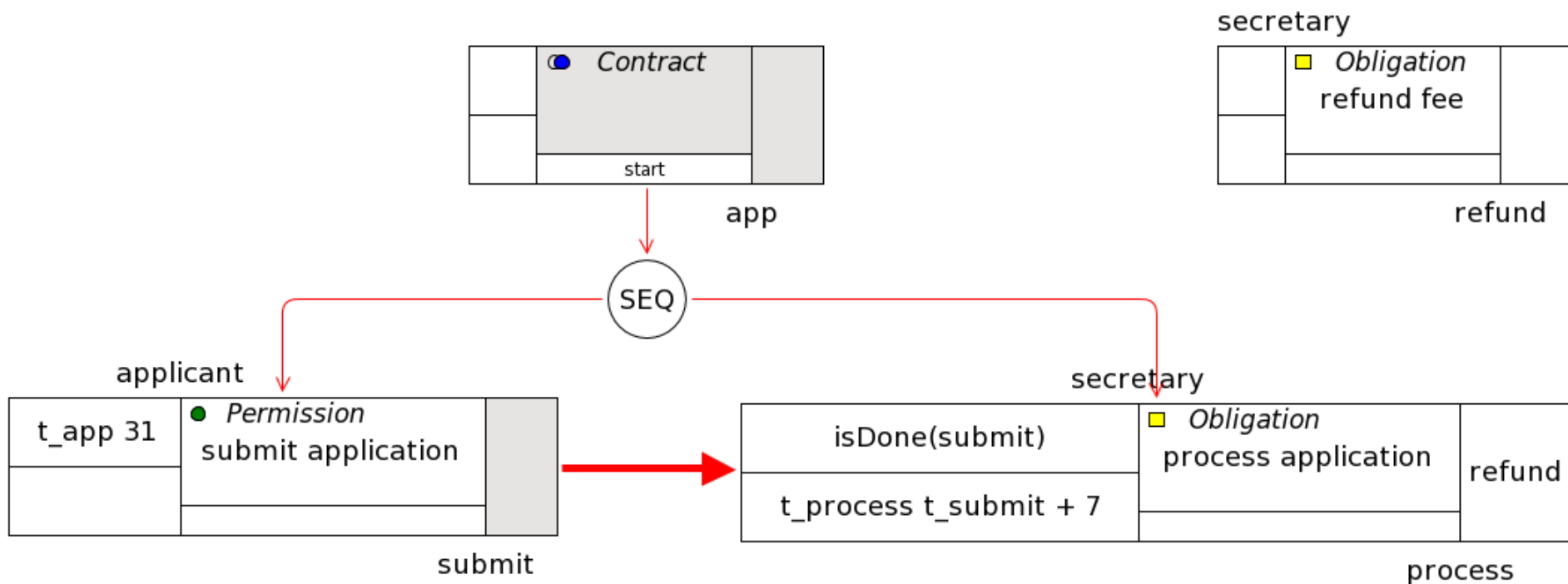
Small steps towards *Contract Analysis*



...the present
(since 2012?)

C-O Diagrams

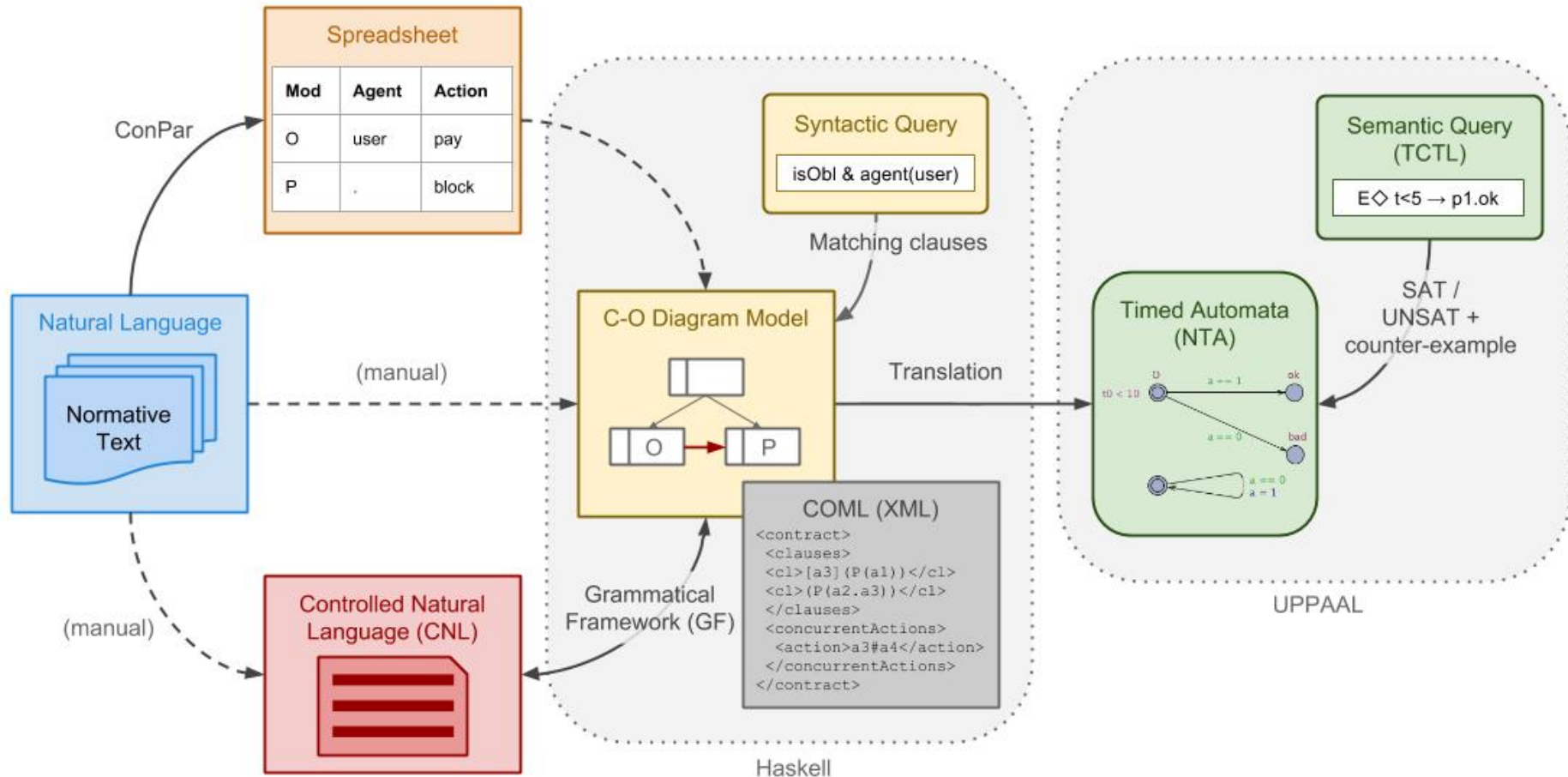
Generalization of CL



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

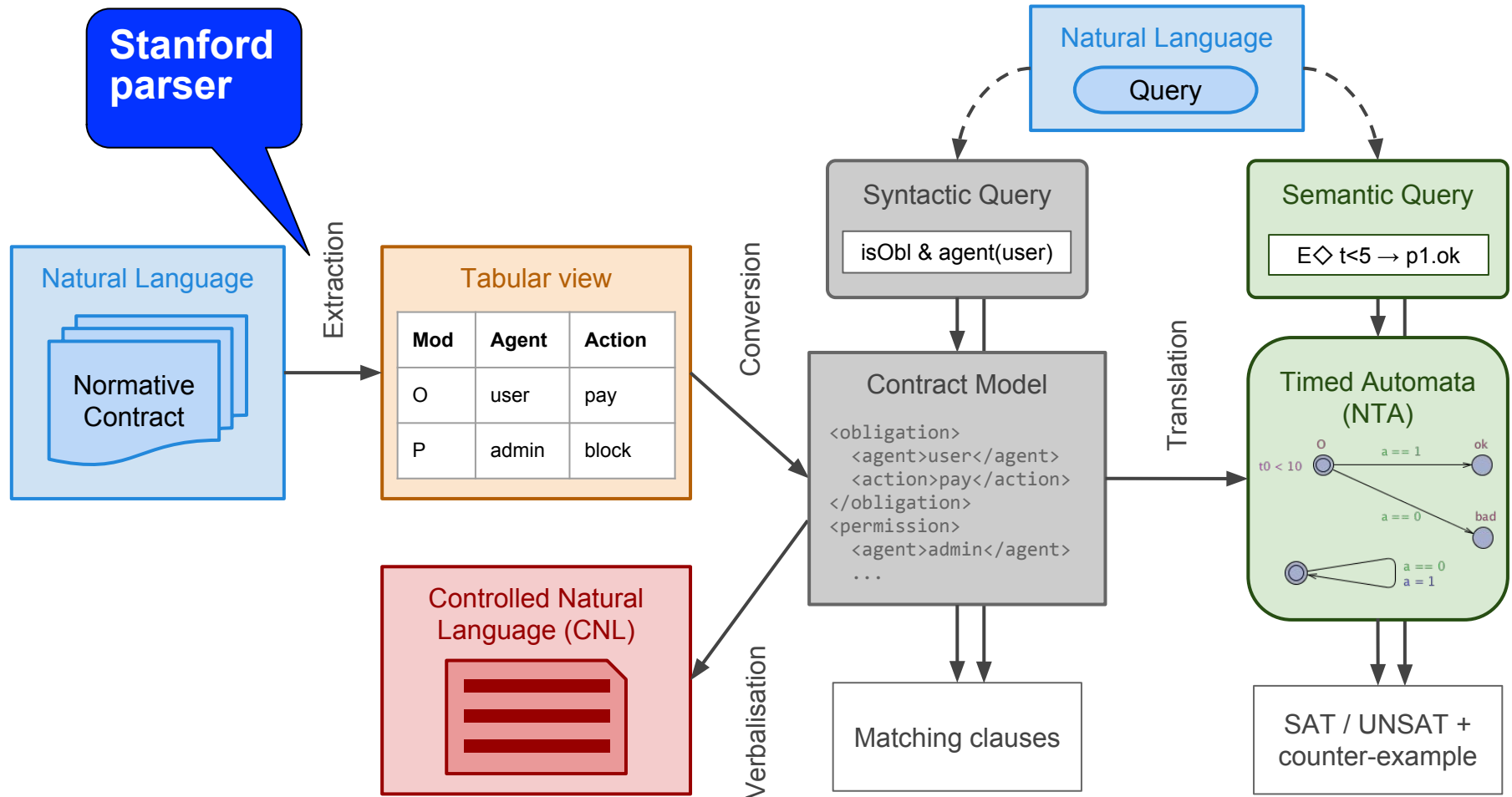
...the present
(since 2012?)

Small steps towards *Contract Analysis*



...the present
(since 2012?)

Contract Verifier. A web based tool for analyzing normative documents



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

* **John J. Camilleri et al** 2016

Contract Verifier

TEXT

Students need to register for the course before the registration deadline , one week after the course has started .
To pass the course , a student must pass both the assignment and the exam .
The deadline for the first assignment submission is on day 10 .
If the submission is not accepted , the student will have until the final deadline on day 25 to re-submit it .
Graders should correct an assignment within one week of it being submitted .
The exam will be held on day 60 .
Students must sign up for the exam at the latest 2 weeks before it is held .

CNL

c1 : when clock t0 is less than 7 student is required to register for course
c2 : all of { - see c2.1 - see c2.2 }
c2.1 : student is required to pass exam
c2.2 : student is required to pass assignment
c3 : when clock t0 is less than 10 student is required to submit assignment
c4 : when clock t0 is less than 25 student is required to submit assignment
c5 : when clock t_c3 is less than 7 grader is required to correct assignment
c6 : student is required to take exam
c7 : when clock t0 is less than 46 student is required to sign up for exam

CODSH

c1:O[t0<7](student.register_for_course)⊥
c2:AND{#c2.1^#c2.2}⊥
~c2.1:O(student.pass_exam)⊥
~c2.2:O(student.pass_assignment)⊥
c3:O[t0<10](student.submit_assignment)⊥
c4:O[t0<25](student.submit_assignment)⊥
c5:O[t_c3<7](grader.correct_assignment)⊥
c6:O(student.take_exam)⊥
c7:O[t0<46](student.sign_up_for_exam)⊥

Different representations of the contract model:

- Original input text (top)
- Controlled natural language (bottom left)
- C-O Diagram (bottom right)

Contract Verifier

Sentence	No	Modality	Subject	Verb	Object	Time	Adverbials	Conditions
<div>✗</div> To pass the course , a student <div>+</div> must pass both the assignment and the exam .	2	AND[2.1,2.2]						
<div>✗</div> <div>+</div>	2.1	O	student	pass	exam		to pass the course	
<div>✗</div> <div>+</div>	2.2	O	student	pass	assignment		to pass the course	
<div>✗</div> The deadline for the first <div>+</div> assignment submission is on day 10 .	3	D	deadline	be [on]	day			DAY: 10
<div>✗</div> If the submission is not <div>+</div> accepted , the student will have until the final deadline on day 25 to re-submit it .	4	O	student	have [until]	final deadline	on day 25		HAVE: if the submission is not accepted
<div>✗</div> Graders should correct an <div>+</div> assignment within one week of it being submitted .	5	{should}	grader	correct	assignment	within one week of <it> being submitted		

- Visualization of the extracted CNL
- Each row indicates a clause (first sentence refined into sub-clauses)
- User can post-edit the extracted output before going on to the next step

Contract Verifier

☐ Who is responsible for [action] ?

☒ What are all the obligations of student ?

☐ What are all the permissions of [agent] ?

☐ What are all the prohibitions of [agent] ?

☐ Are there obligations without reparation?

☐ Are there prohibitions without reparation?

☐ Is the contract satisfiable?

☒ The student must pass exam in order for the contract to be satisfied.

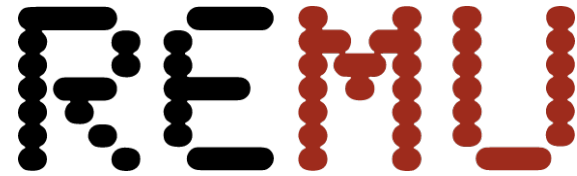
☐ The [agent] must [action] before [] time units.

☐ Is it required that [agent2] does [action2] within [] time units after [agent1] does [action1] ?

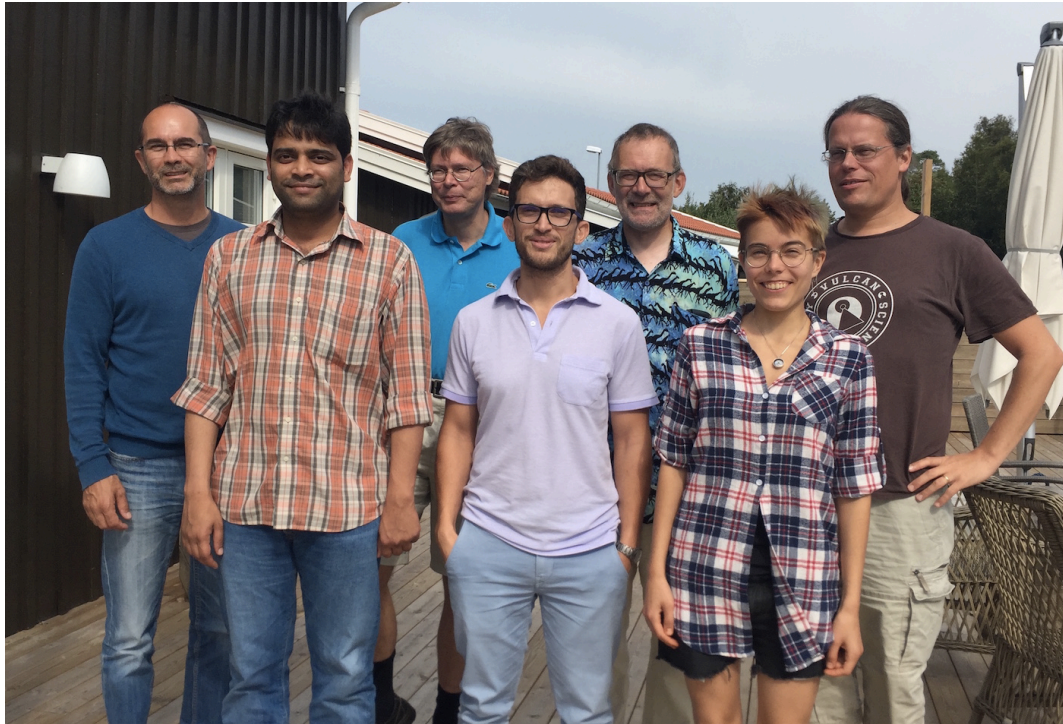
Automatic
extraction of
actions and
actors

Syntactic and
"semantic"
queries

- Queries
 - Syntactic (text mining on the internal xml representation)
 - "Semantic" (timed automata -> UPPAAL)



Reliable Multilingual Digital Communication: Methods and Applications

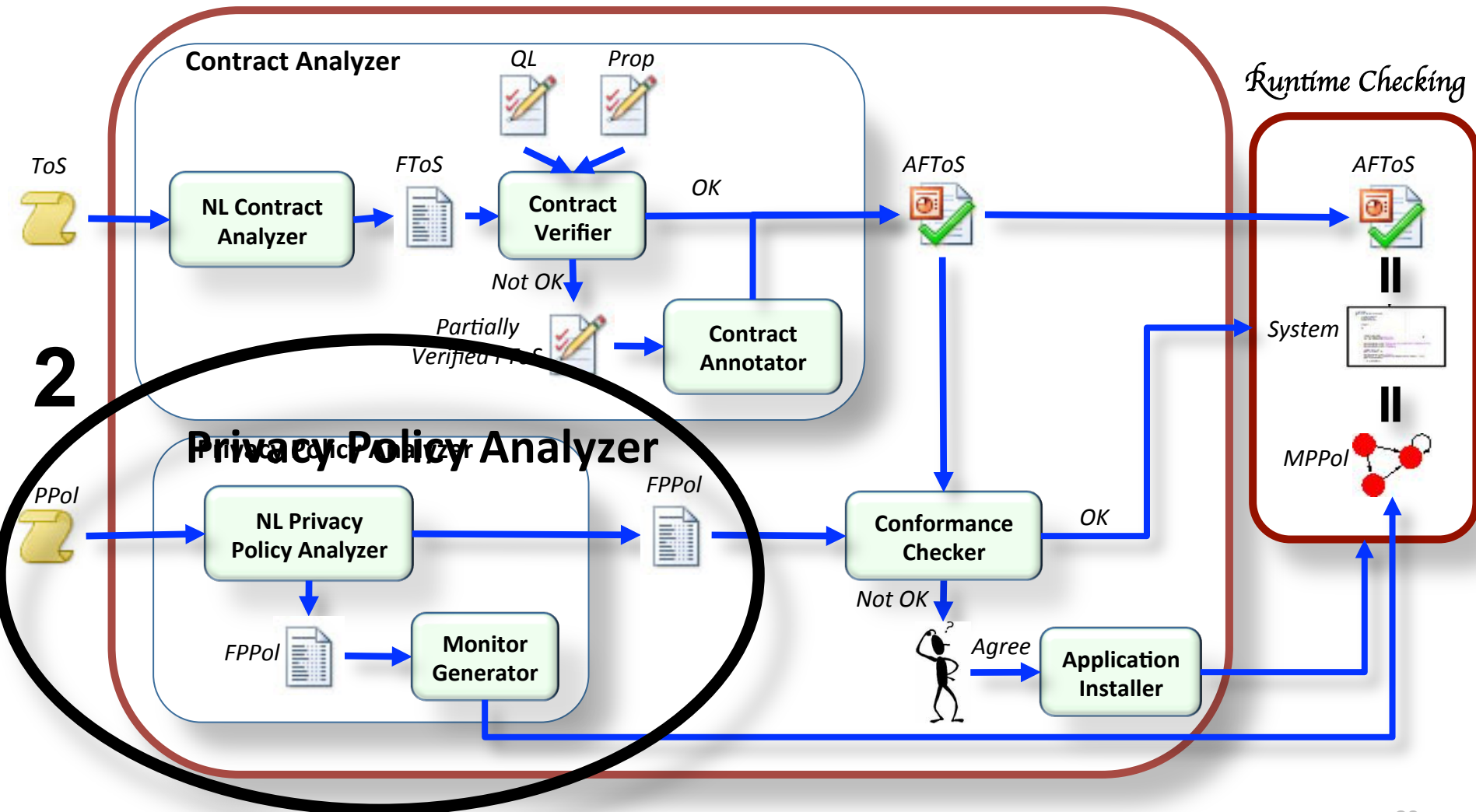


<http://remu.grammaticalframework.org/>



Vetenskapsrådet

Privacy-Preserving Contractual Agreement Framework




Privacy Policies

What have we done so far?

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

PPF: Privacy Policy Framework

- 
- The diagram shows three blue chevron arrows pointing to the right, each pointing to a box containing a component of the PPF framework.
- PPL – Privacy Policy Language
 - KBL – Knowledge-Based Logic
 - Knowledge Base

Interpreted over ***Social Graphs***

For Social Networks

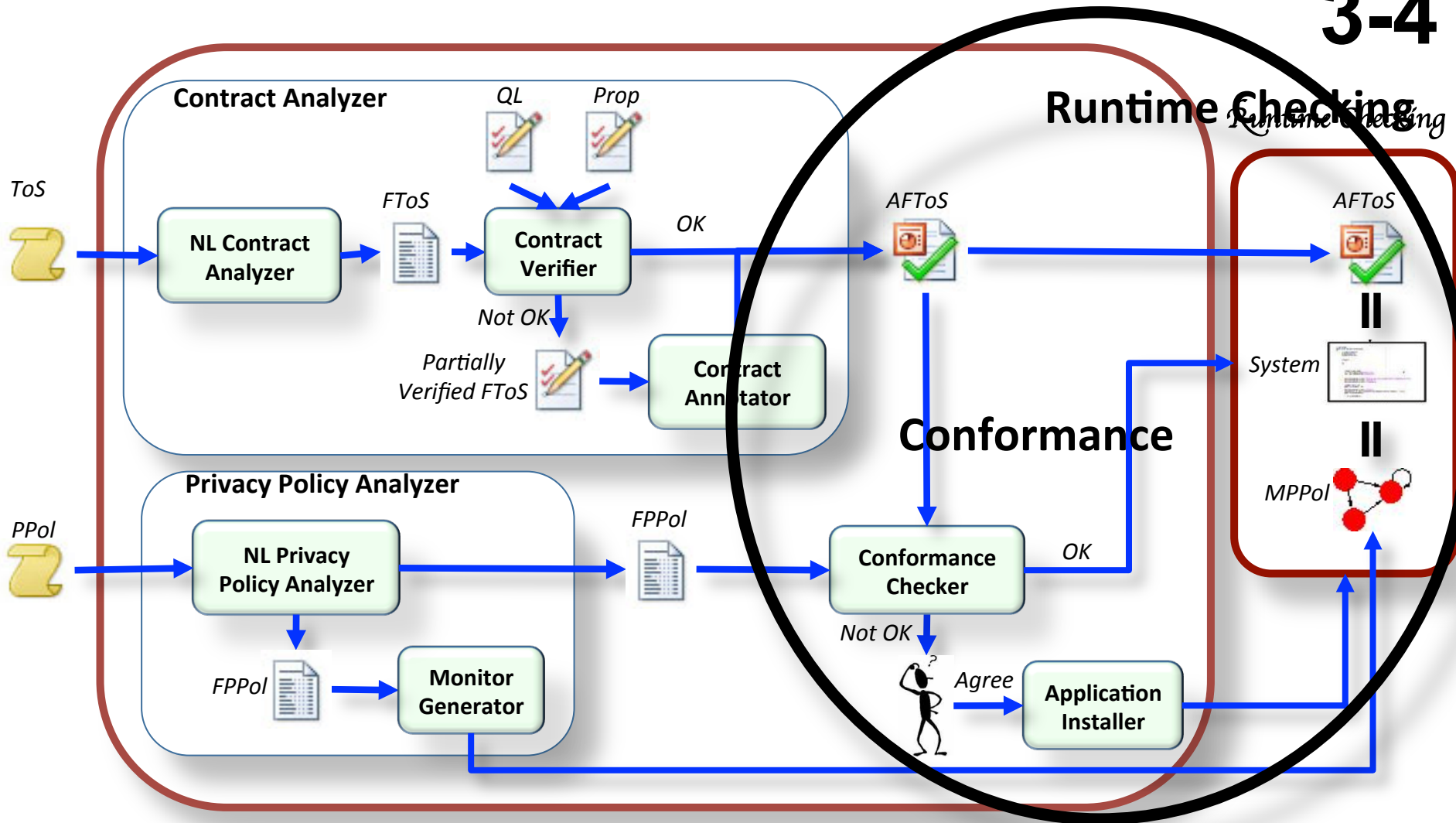
"Evolving" policies:

- Automata
- Real-Time

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

Privacy-Preserving Contractual Agreement Framework

3-4



Conformance Checking ***Runtime Checking***

What have we done so far?

Not much...

“Contracts” or Runtime Checking

- Runtime Enforcement of Evolving Privacy Policies in OSN (using Policy Automata)
 - Joint work with R. Pardo, C. Colombo and G. Pace,
- Runtime monitoring of browser extensions based on privacy policies
 - Joint work with R. Pardo, P. Picazo-Sánchez and J. Tapiador

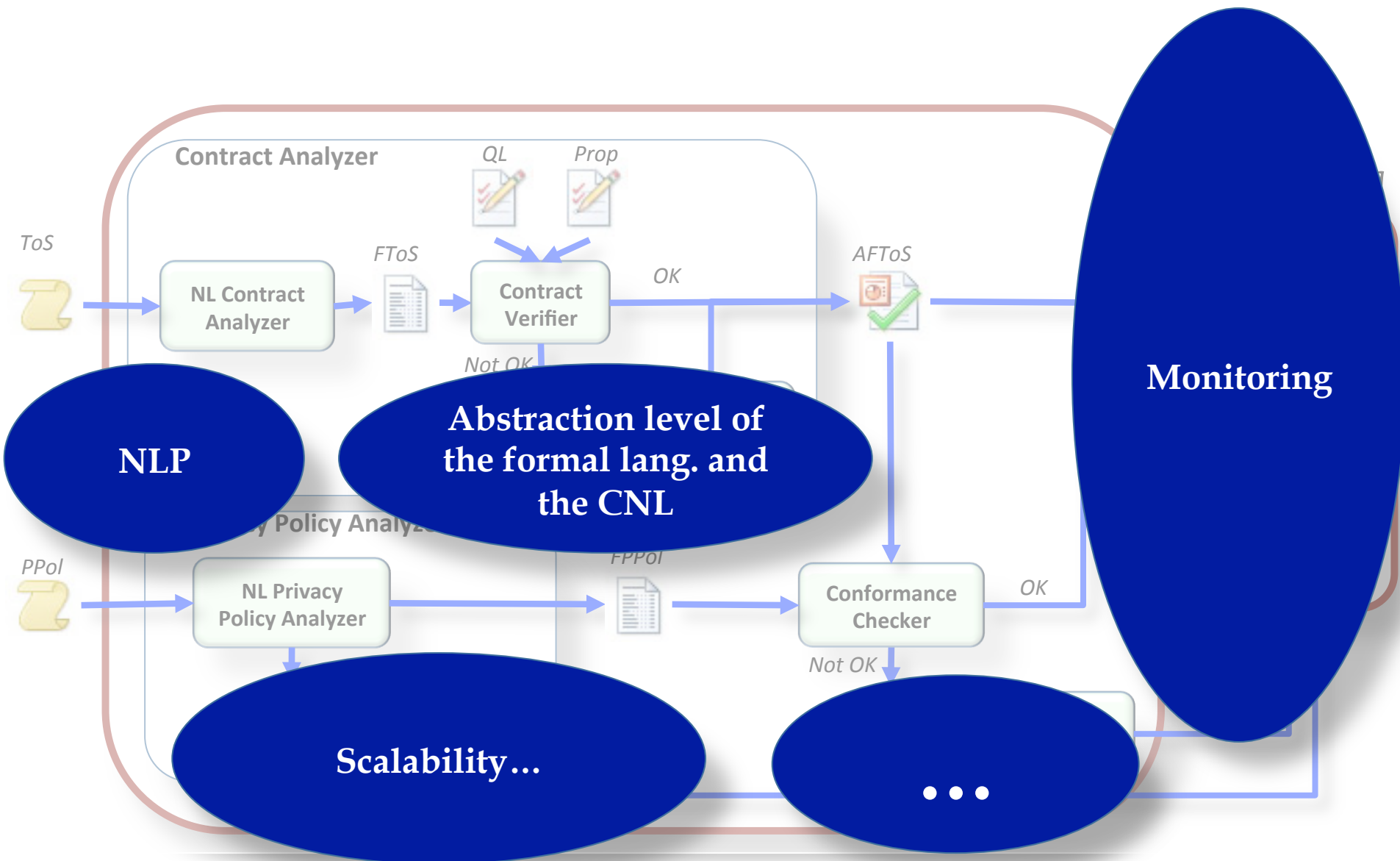
“Contracts” but not RV:

- Contract Automata
 - Joint work with G. Pace, F. Schapachnik, S. Azzopardi
- A CNL for railway station regulations
 - Joint work with B. Luterberget, J.J. Camilleri, C. Prisacariu

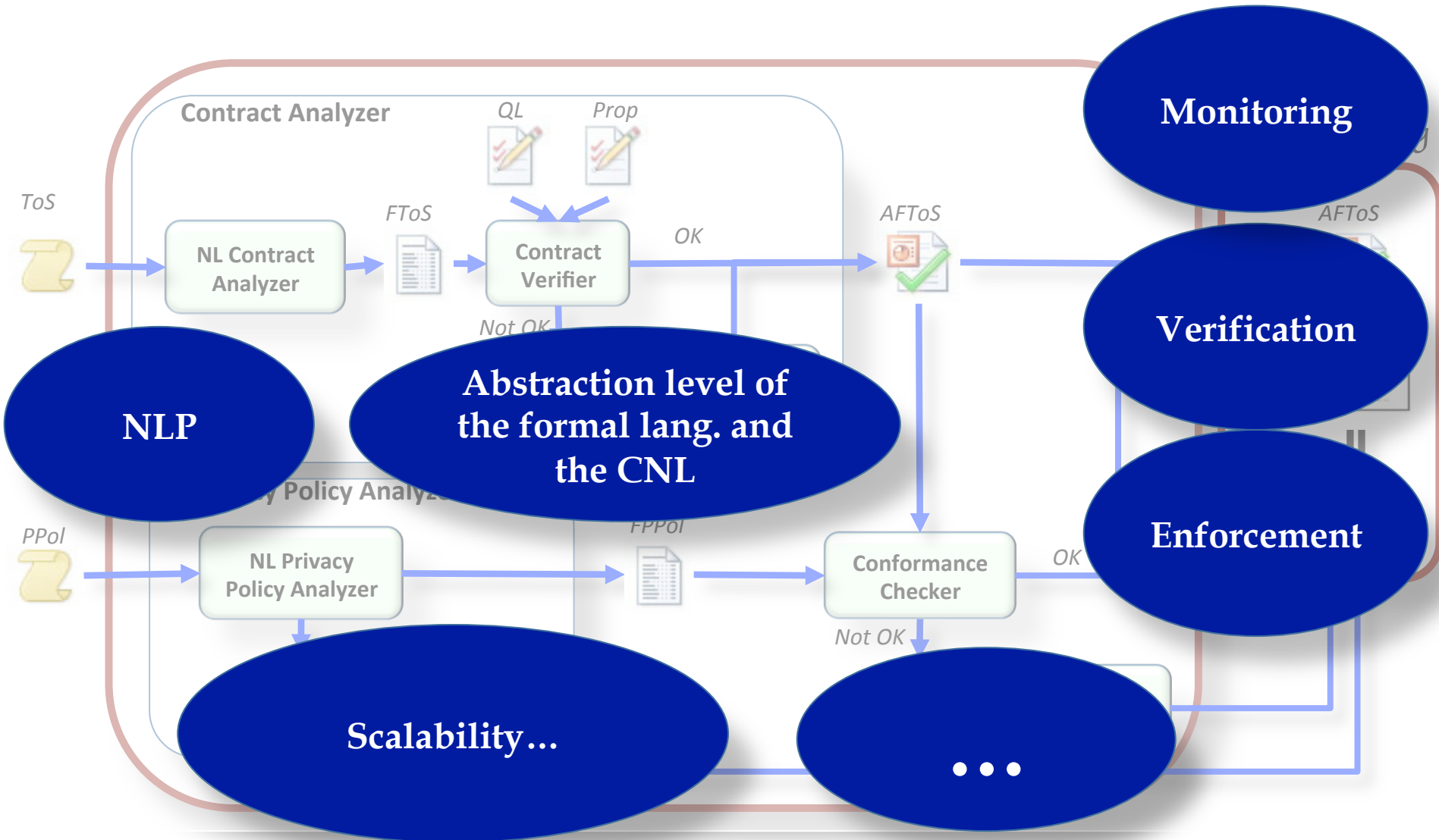
RV but not “contracts”:

- Secure migrating monitors for the IoT
 - Joint work with P. Picazo-Sánchez and G. Pace
- And of course... StarVOOrS
 - Joint work with W. Ahrendt, M. Chimento and G. Pace

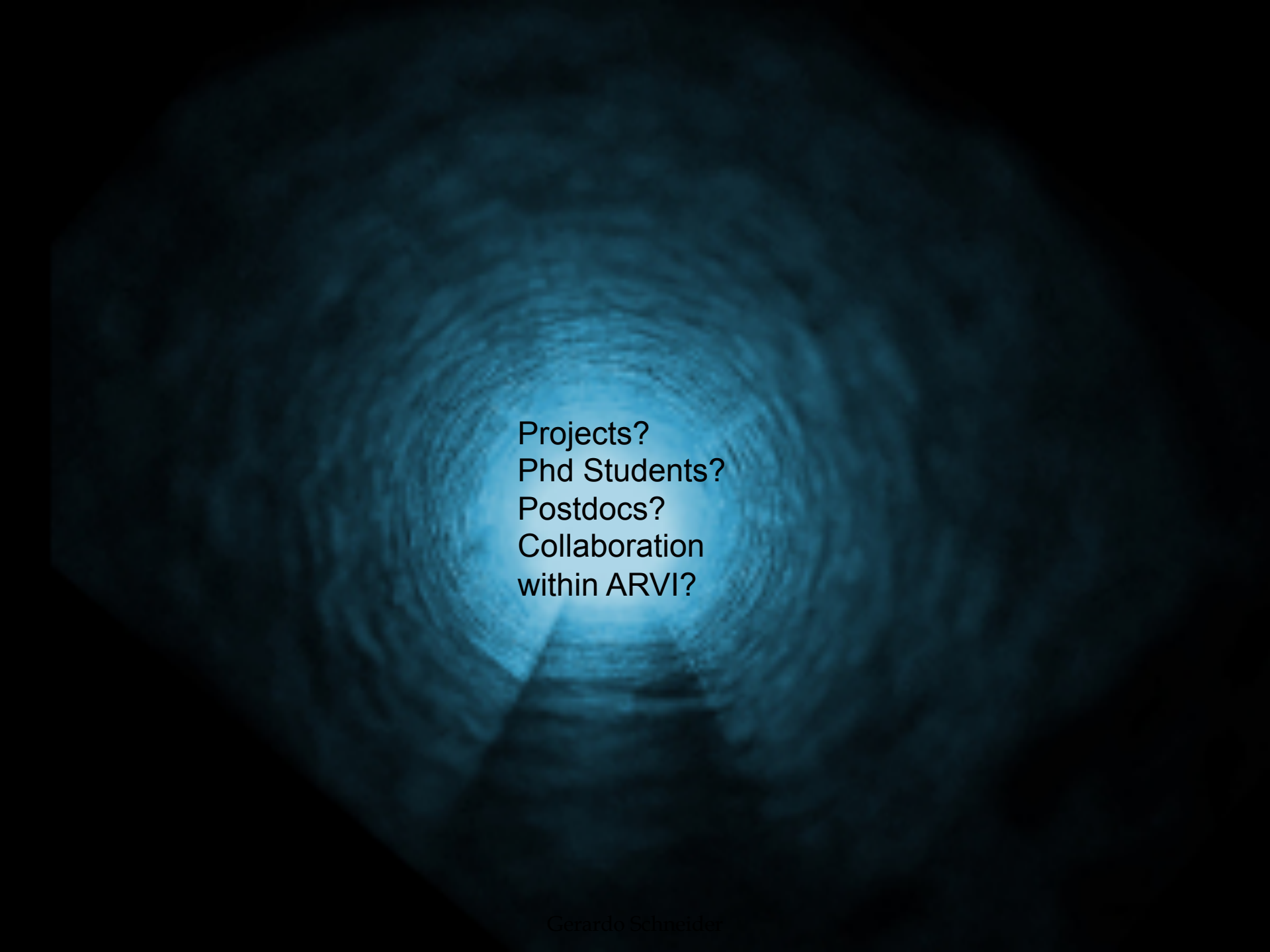
A lot of challenges!



A lot of challenges!

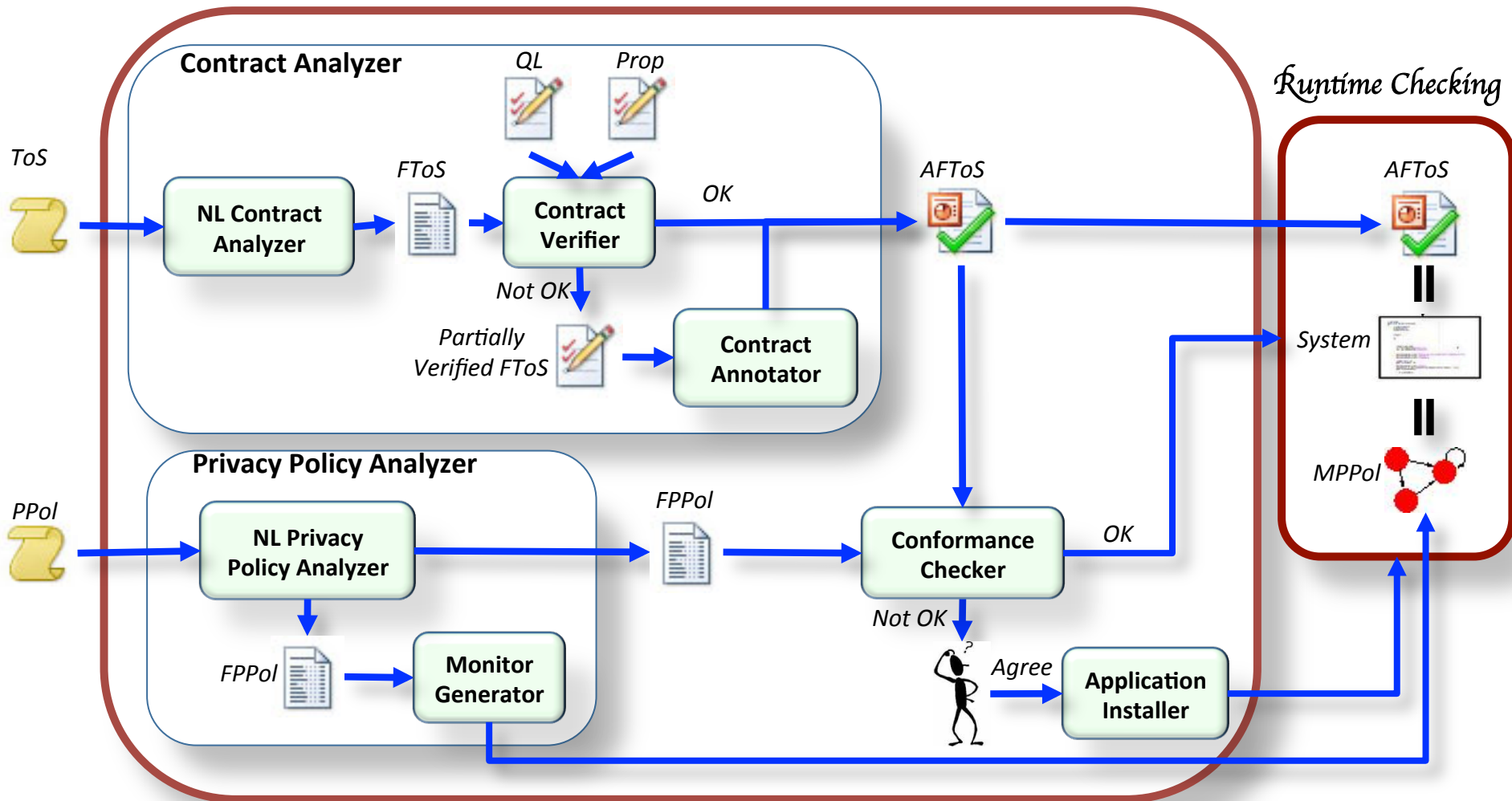






Projects?
Phd Students?
Postdocs?
Collaboration
within ARVI?

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

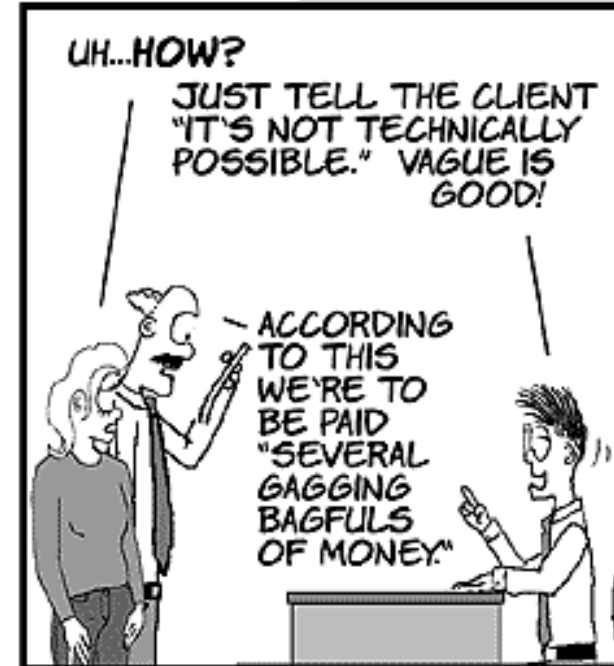
“for their contributions to **contract theory**”



USER FRIENDLY by J.D. "Illiad" Frazer

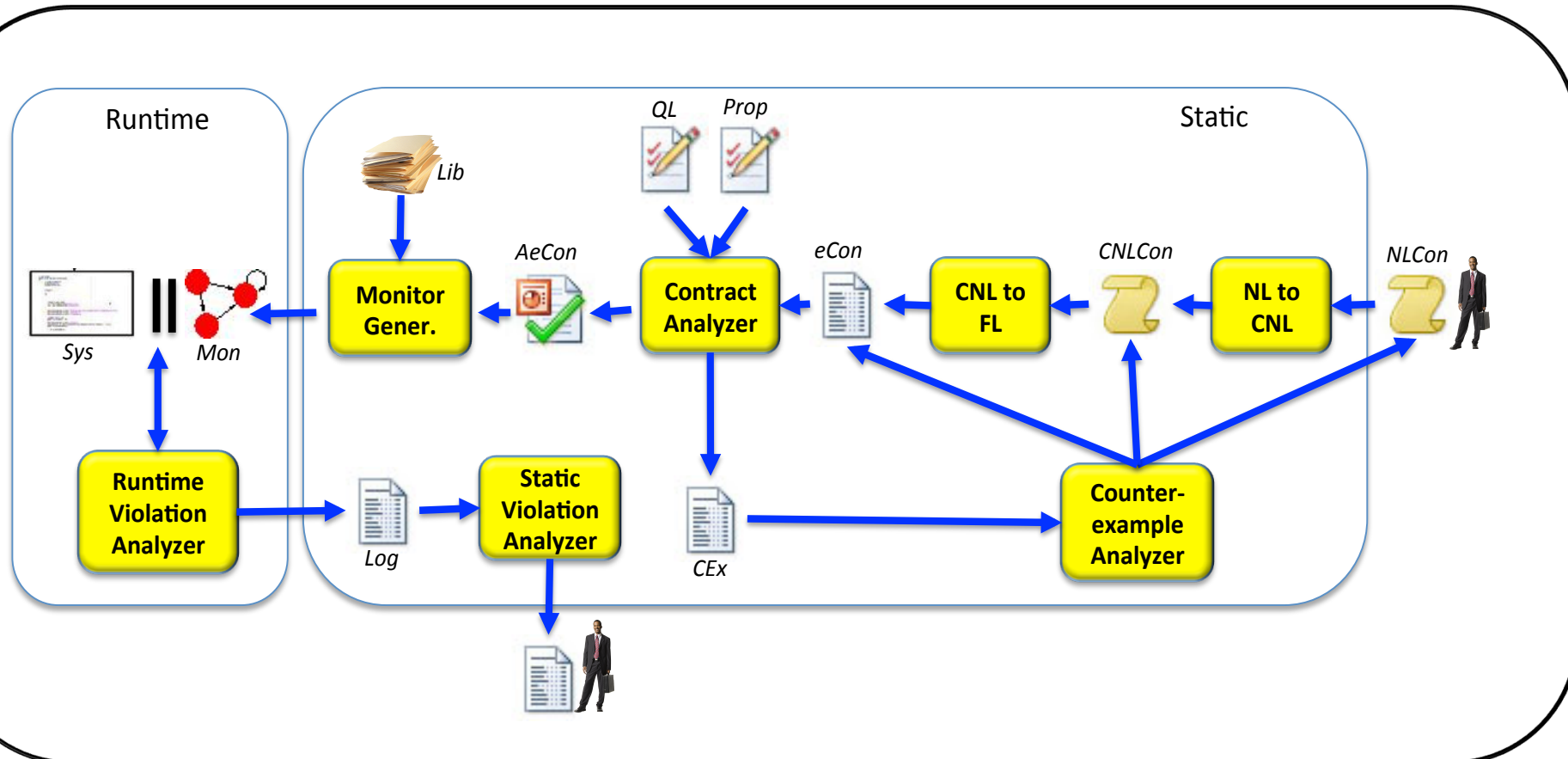


(THIS 'TOON IS A REPEAT)



Auxiliary Slides

Contract Analysis... revisited realistically



Many challenges to address before getting a fully working system!

- Will mention few of them...

Contract Analysis... revisited realistically

