



Verification and Validation of Electronic Contracts

Carlos Molina-Jimenez

Carlos.Molina@ncl.ac.uk

Newcastle University, UK

Red Hat Research Day

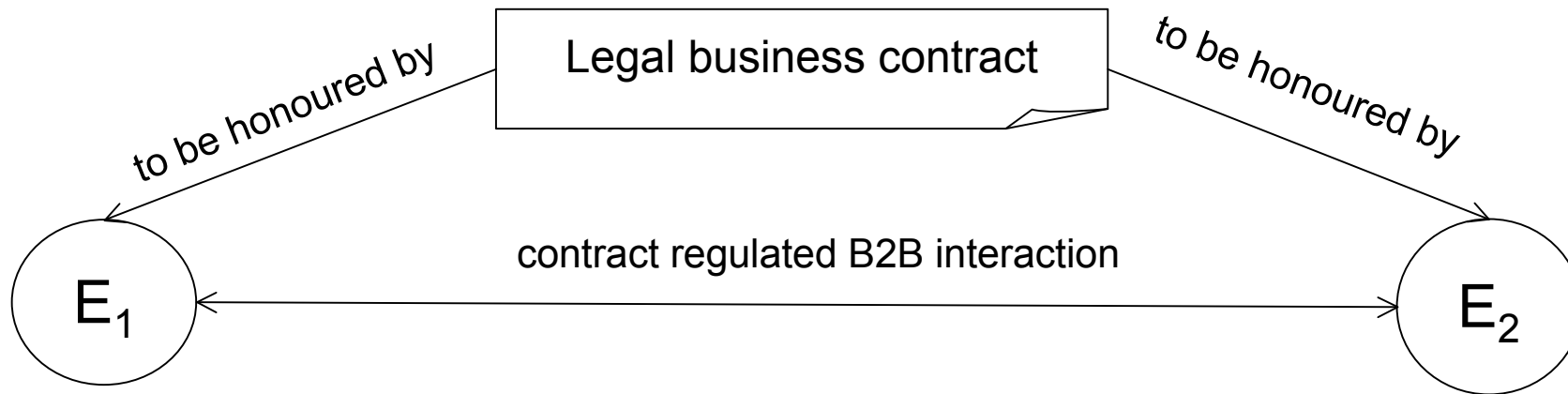
Newcastle University,

Aug 15, 2011

Outline of the topic

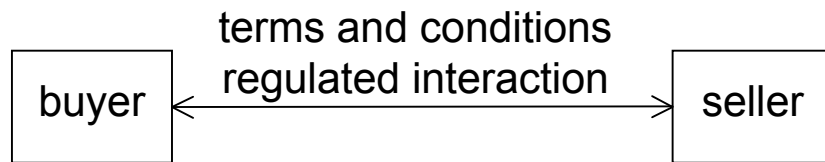
- General picture: Contractual business interactions.
 - Contracts as mechanisms to prevent and solve disputes.
- Terms and conditions and SLAs.
- Example of a Term and Conditions contract.
- Rights, obligations and prohibitions.
- Contract monitoring and enforcement.
- Implementation of correct contracts.
- Intuitive contract notation.
- Contingency clauses.
- Logical inconsistencies in contractual clauses.
- Verification of contractual clauses with model-checking.
- Validation of contract implementation with model-checking generated test cases.
- Questions and discussion.

The general picture



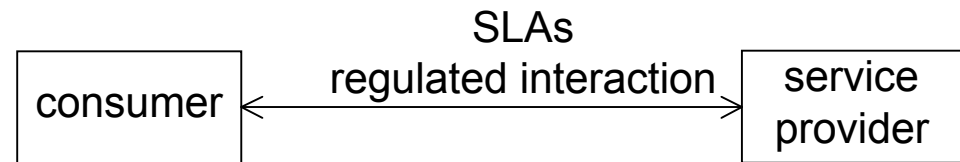
- E₁ and E₂ are two autonomous and independent business enterprises (companies).
- They've decided to conduct business over the Internet.
- They do not trust each other unguardedly.
 - They rely on a legal business contract to help them prevent misunderstanding and solve potential disputes.

Terms and Conditions and SLAs interactions



a)

- Buyer obliged to submit payment within 3 days of receipt of the purchase order.
- Seller permit to reject payments by questionable credit cards.



b)

- Consumer permitted to place up to 10 requests per second.
- Provider obliged to keep the service operational 7 days a week.

Ex 1: conventional contract (Perrin'04)

- 1. The travel agency can send ticket offers to the customer.*
- 2. The offer should be delivered by the Dec 15, 2007. The offer can be delivered more than one times before this date.*
- 3. The customer should accept one offer by the December 31, 2003. The acceptance can be done only once.*
- 4. Payment by credit card is due within seven days after acceptance.*
- 5. Payment by credit card is retriabile twice.*
- 6. If payment by credit card fails, another payment mean is accepted, but only once.*
- 7. The items must be sent to the customer within four days after the payment is validated by the bank.*

Abstraction of contract clauses: Rights, Obligations and Prohibitions

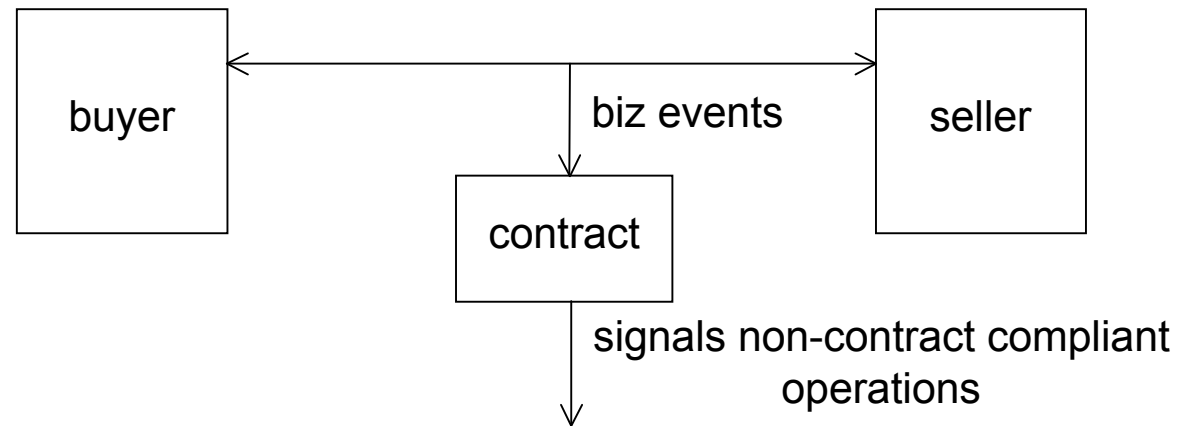
- Right (R) : an action that a business partner is allowed to do if he or she wishes to.
- Obligation (O): an action that a business partner is expected to do.
 - Failure to executed the action might result is economical sanctions.
- Prohibition (F): an action that a business partner is forbidden to do.
 - The execution of a forbidden action might result in economical sanctions.
- Actions are biz operations stipulated in the contract clauses: send a purchase order, place payment, cancel purchase order, etc.

The Challenge

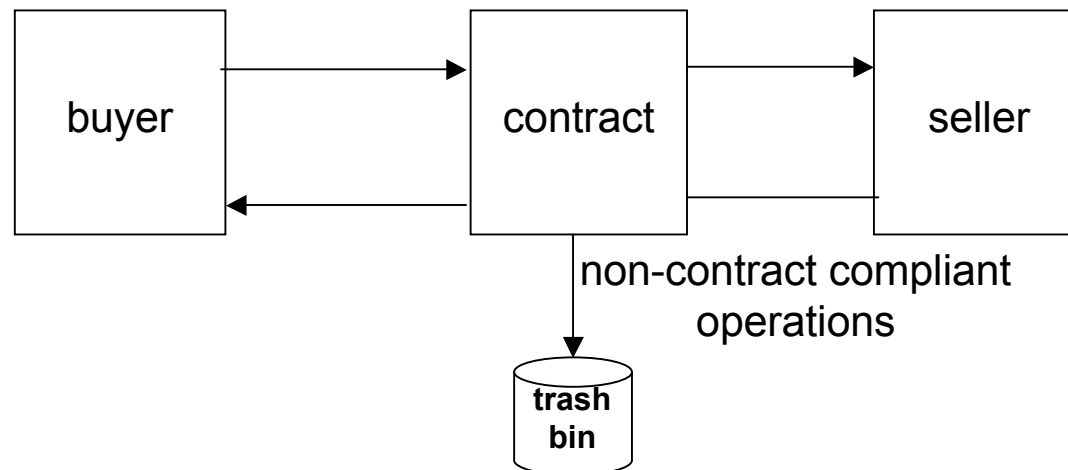
- How to detect and prevent potential violations of the contract?

Contract Monitoring and Contract Enforcement

A) Contract monitoring



B) Contract enforcement



How to implement a correct (executable) contract? --4 goals

1. Contract clauses should be intuitively expressed.
 - An intuitive to read, understand and write notation is desirable.
2. Contract clauses should count for exceptional situations.
 - *Buyer will be granted 3 days deadline extension to pay if timely payment failed due to technical reasons.*
3. No logical inconsistencies in the clauses.
 - *The buyer is obliged and prohibited to pay.*
4. No implementation errors in the actual code.

1) Intuitive ECA-notation

- We use a notation inspired by the Event Condition Action (ECA) notation.
- We found ECA notation to be intuitive and expressive enough to encode most (all?) typical business clauses.
- Ex.

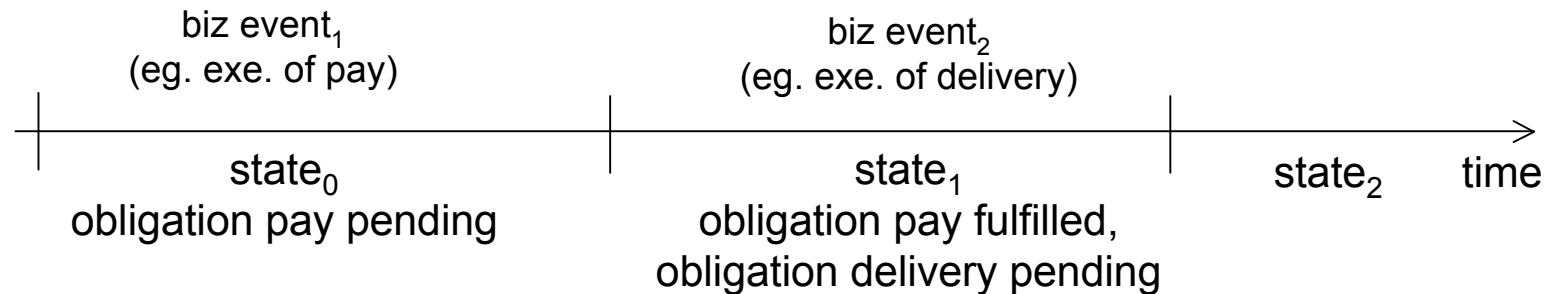
event: *payment submitted by buyer.*

cond: *timely payment.*

action: *impose obligation to deliver within 7 days on seller.*

ECA-rules with Rights-Obligations-Prohibitions Centric View

The interaction can be regarded as a sequence of states



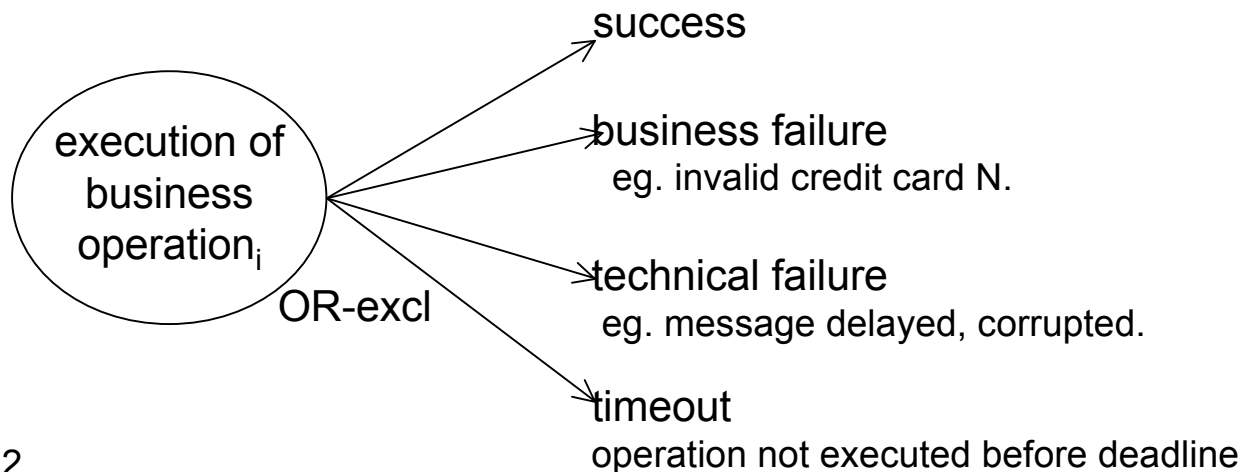
- In a Rights-Obligations-Prohibitions (ROP) centric view a contract stipulates what operations parties have the **right**, **obligation** or **prohibition** to execute in each state.
- Rights, obligations and prohibitions become **enabled** and **disabled** as the interaction progresses through its states.
- So, in each state a party has a right/obligation/prohibition when the right/obligation/prohibition is enabled.

2) Contingency clauses (exception handling)

- In an idealised scenario the execution of a given operation always complete successfully.
- In practice “success” is only one of several possible outcomes.
 - We distinguish four.
 - In our ECA language, we can account for these four potential outcomes.
 - We can encode contingency clauses like:

Clause Plan-A: *If buyer does not pay in time, fine him unless.*

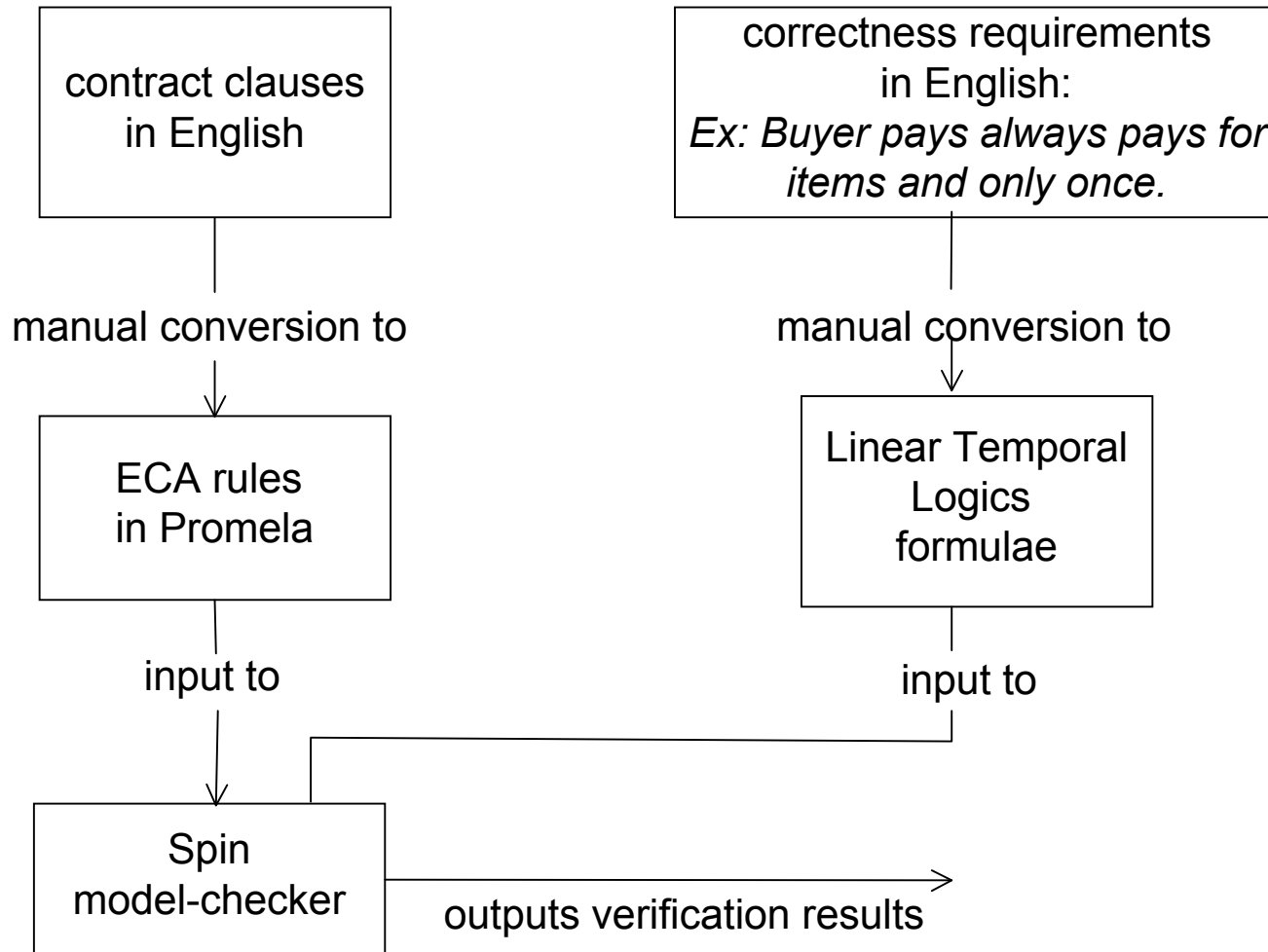
Clause Plan-B: *He does not pay in time due to technical or biz problems, in this case do not fine him, but grant him 3 day extension.*



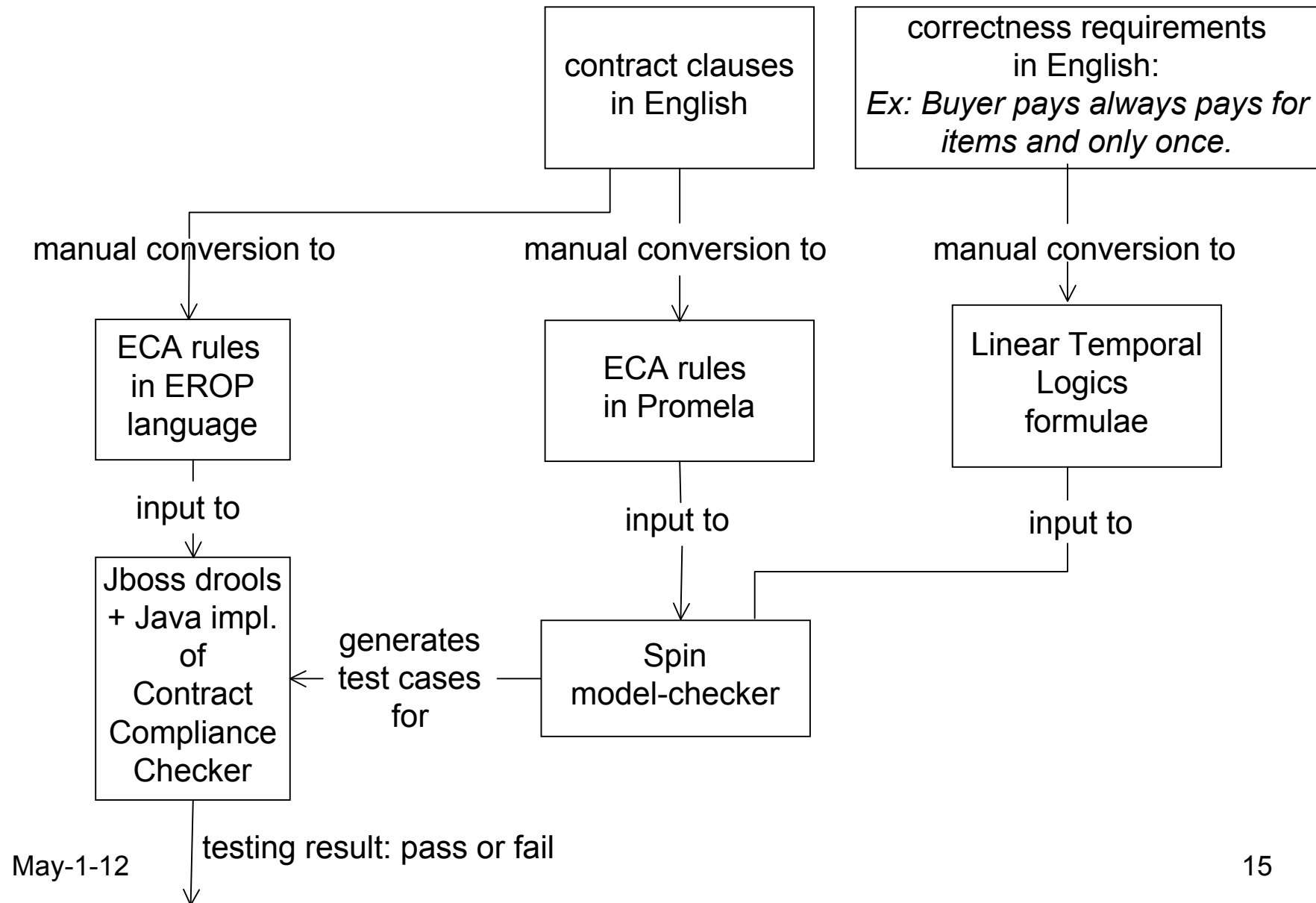
3) Logical inconsistencies in contract clauses

- The intended meaning of contract clauses expressed in natural language can be hard to capture and encode in concise notation.
- Ambiguity, omission, redundancy, contradiction and similar logical errors are likely to impact the contract.
- Contract verification (eg, model-checking) is desirable.
- We have been exploring the suitability of the model-checker Spin in the verification of contract clauses.

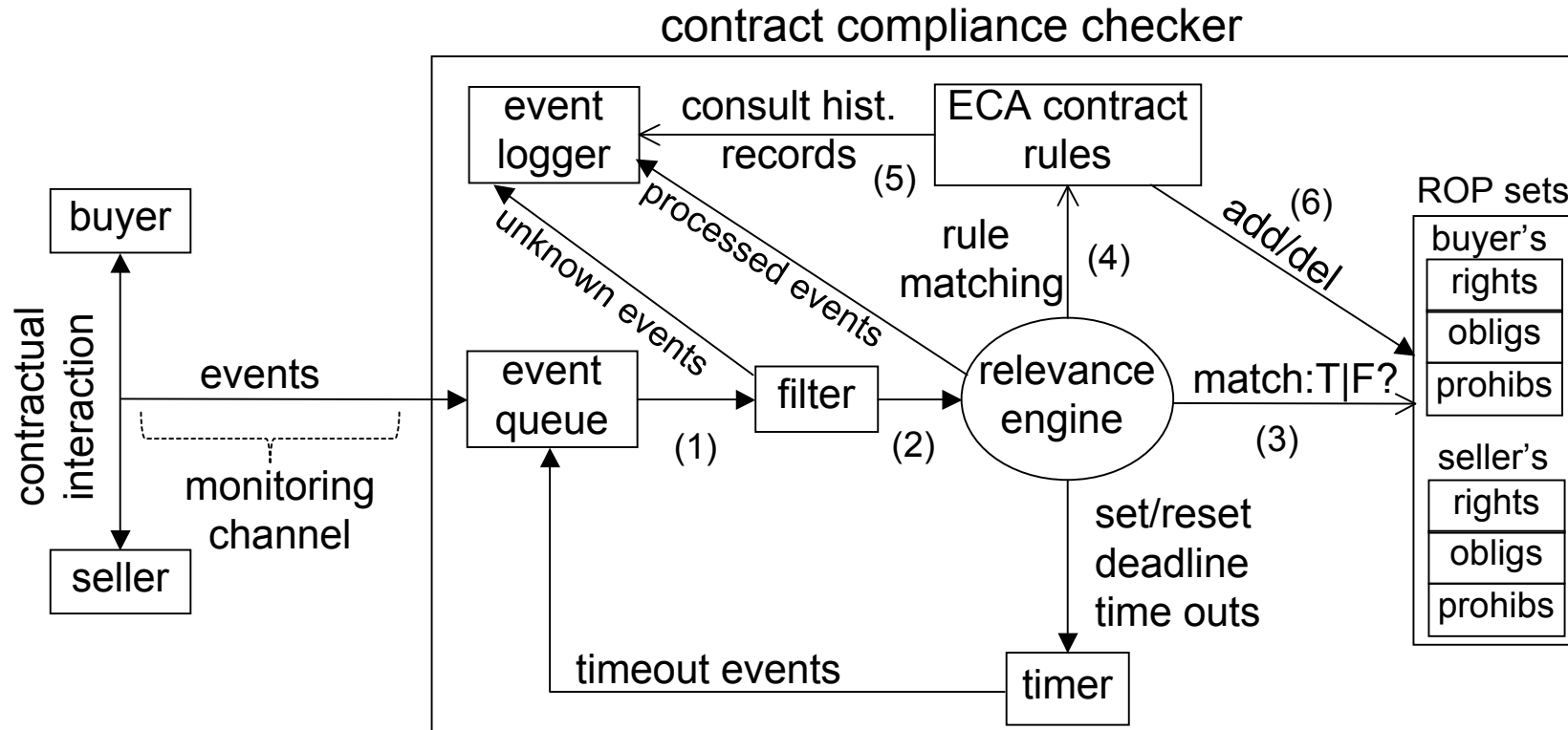
Spin verification



Spin validation (model-checking based testing)



Current implementation: Contract Compliance Checker



Questions and discussion

- Any question (directly or remotely related to the topic) is welcome.

References

- C. Molina-Jimenez, S. Shrivastava, and M. Strano, “A model for checking contractual compliance of business interactions,” *IEEE Tran. on Service Computing*, vol. PP, no. 99, 2011.
- M. Strano, C. Molina-Jimenez, and S. Shrivastava, “Implementing a rule-based contract compliance checker,” in *Proc. 9th IFIP Conf. on e-Business, e-Services, and e-Society (I3E’2009)*. Nancy, France: Springer, 2009, pp. 96–111.
- A. Abdelsadiq, C. Molina-Jimenez, and S. Shrivastava, “On model checker based testing of electronic contracting systems,” in *12th IEEE Int’l Conf. on Commerce and Enterprise Computing(CEC’10)*, 2010, pp. 88–95.
- C. Molina-Jimenez and S. Shrivastava, “Model checking correctness properties of a middleware service for contract compliance,” in *In Proc. of the 4th Int’l Workshop on Middleware for Service Oriented Computing (MW4SOC’09)*. Nov. 30, Urbana–Champaign, USA: ACM digital library, 2009, pp. 13–18.