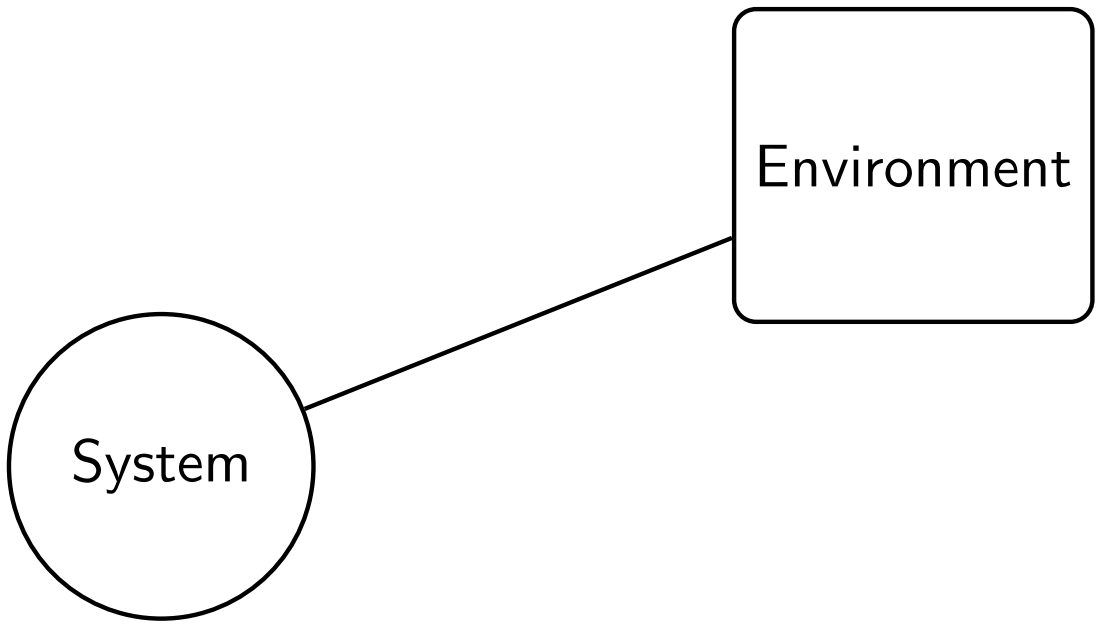
Symbolic vs. Bounded Synthesis for Petri Games

Bernd Finkbeiner[1], Manuel Gieseking[2],
Jesko Hecking-Harbusch[1], Ernst-Rüdiger Olderog[2]

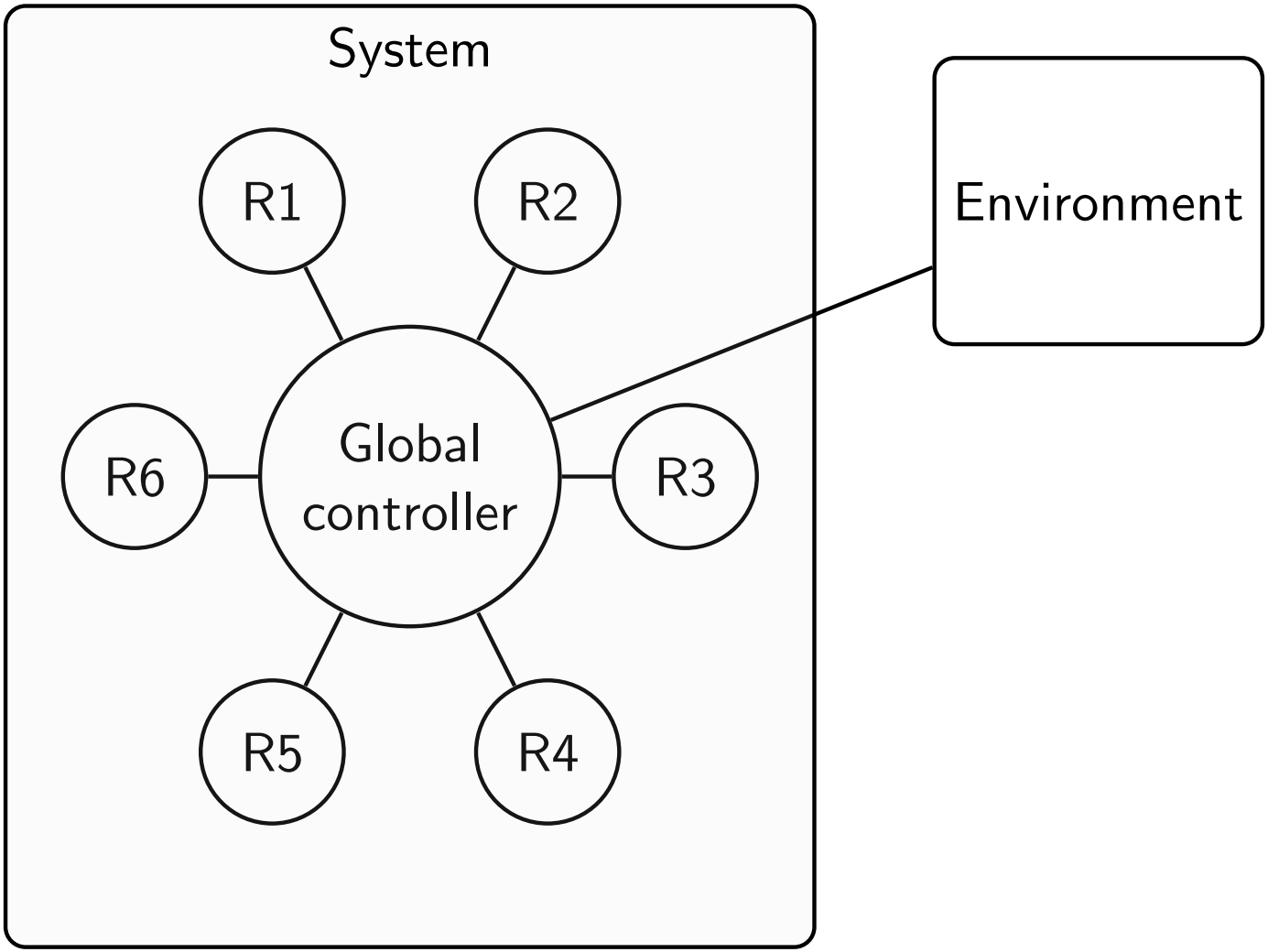
[1]Universität des Saarlandes
[2]Carl von Ossietzky Universität Oldenburg

SYNT, July 22, 2017

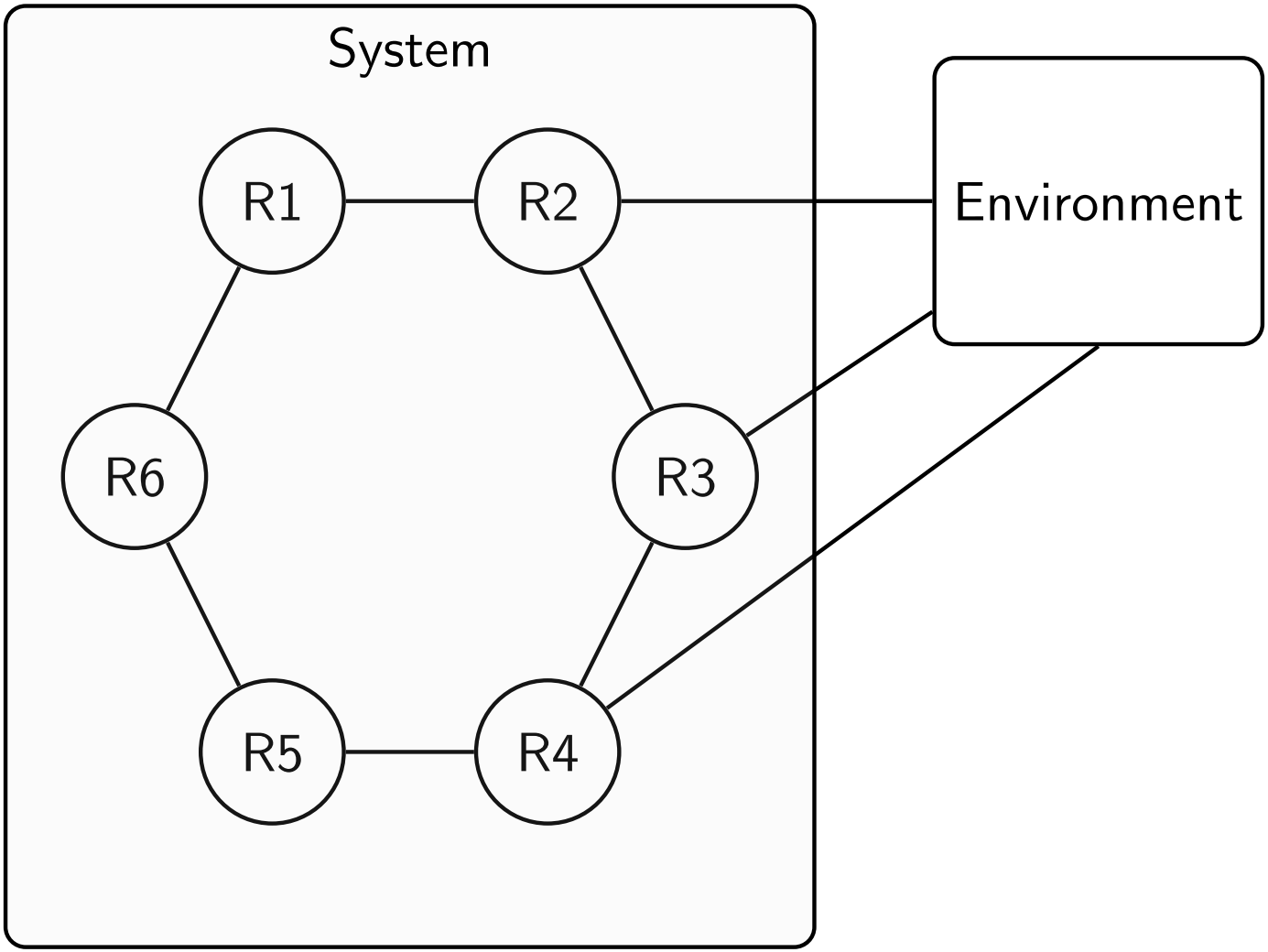
Synthesis



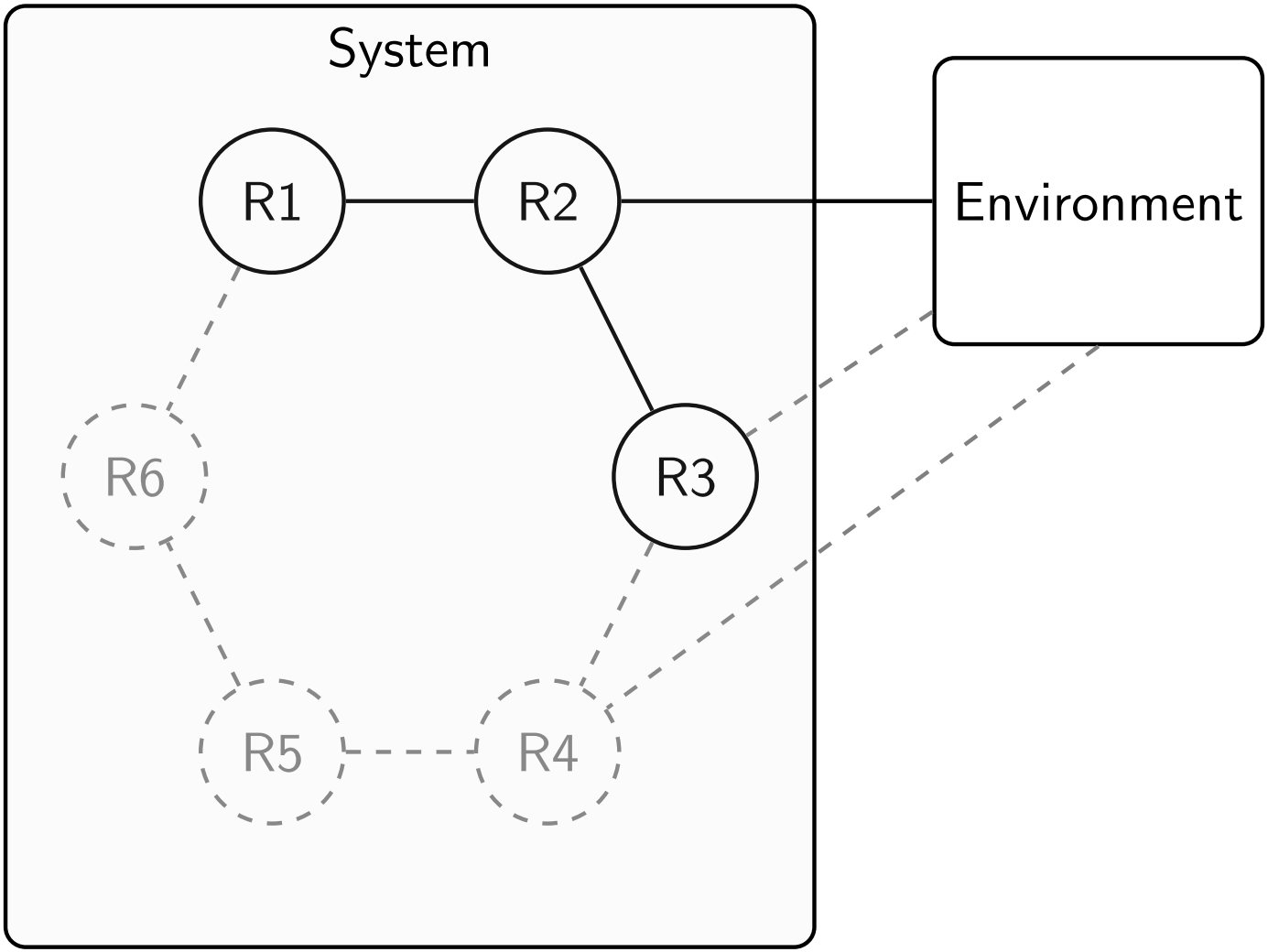
Synthesis



Distributed Synthesis



Local Information



Distributed Synthesis with Petri Games [Finkbeiner, Olderog, '14]

Existing tool:

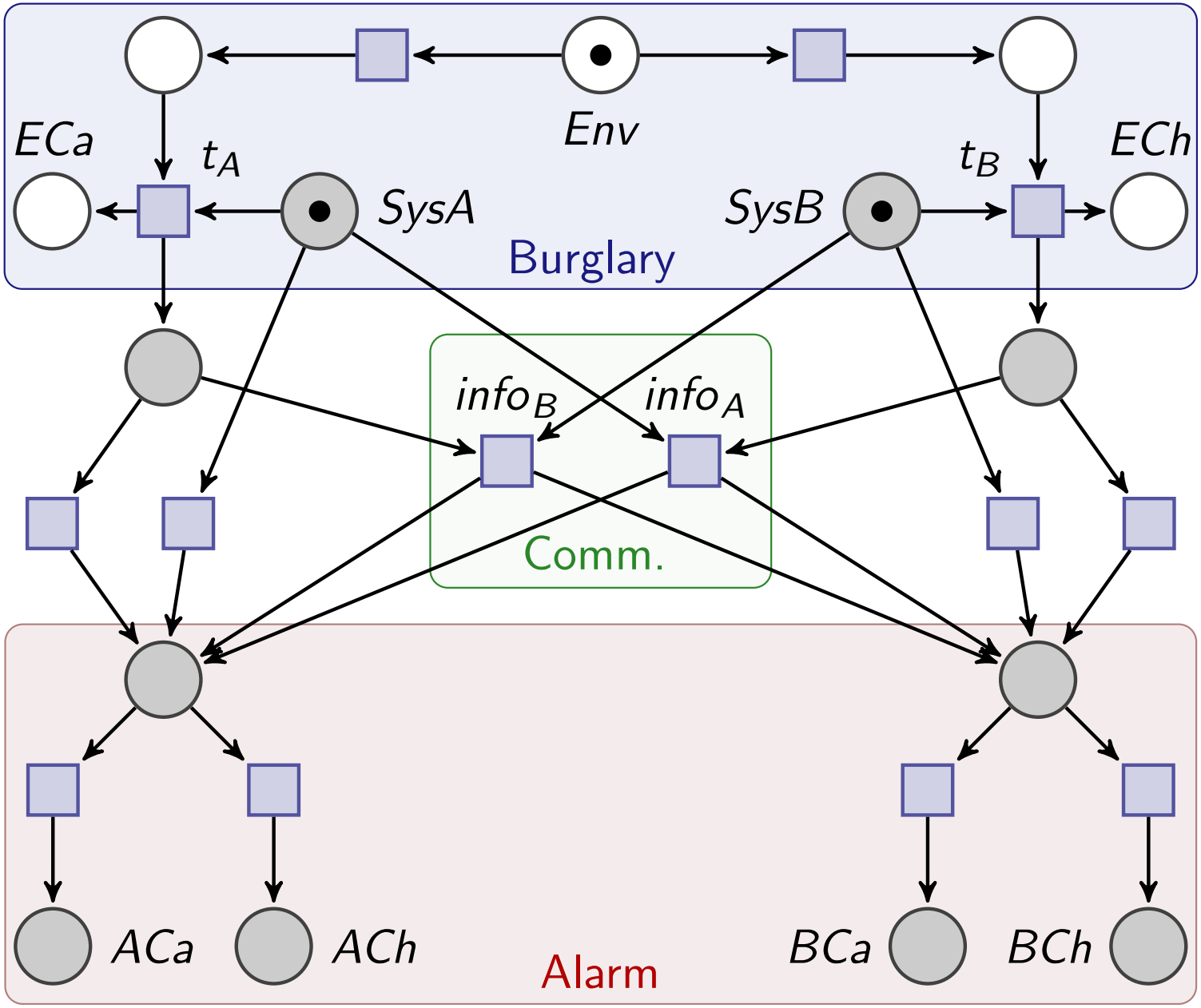
- ADAM is used to synthesize Petri games *symbolically*.

New tool:

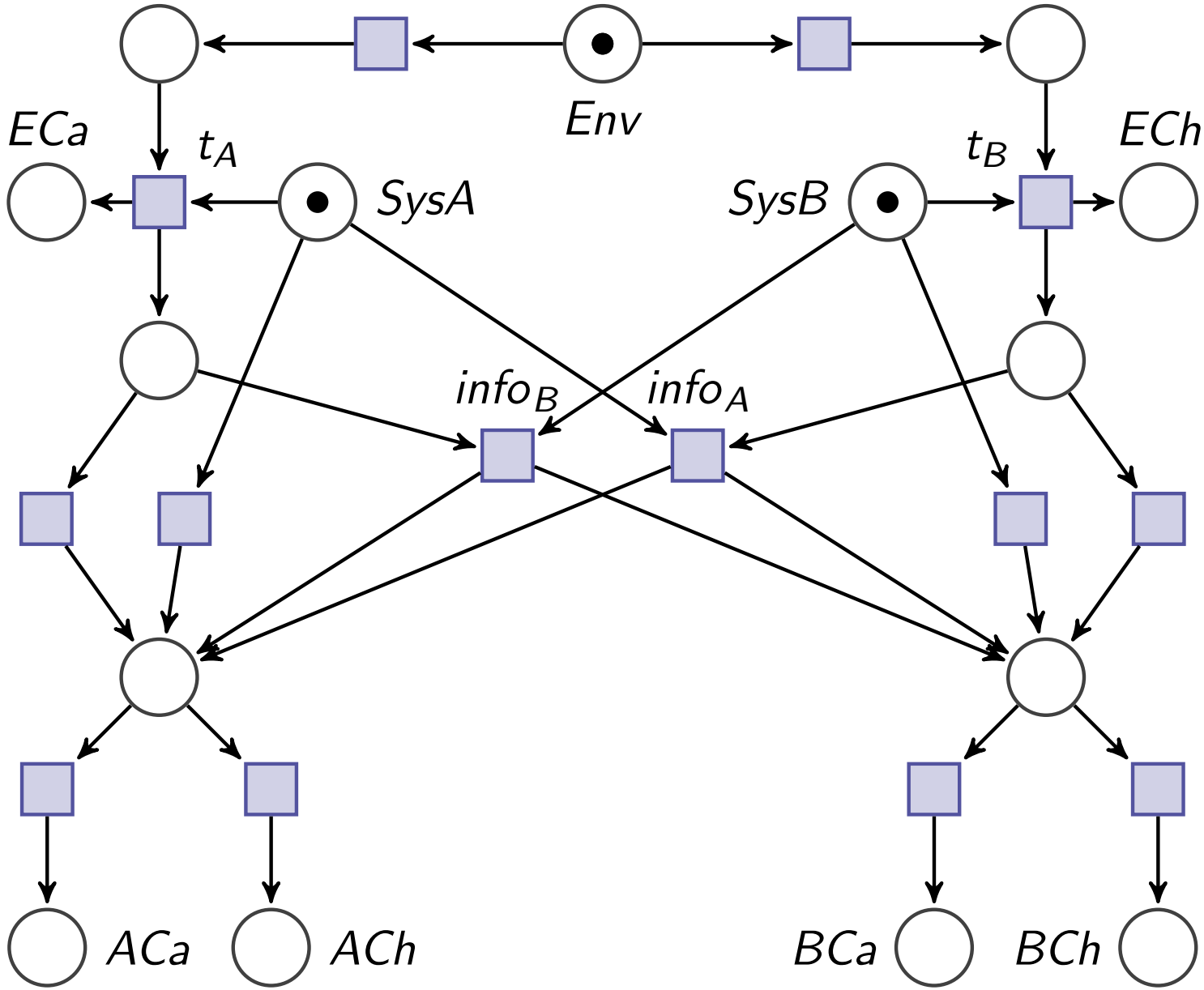
- Prototype implementation of *bounded synthesis*.

We compare experimental results of the two approaches.

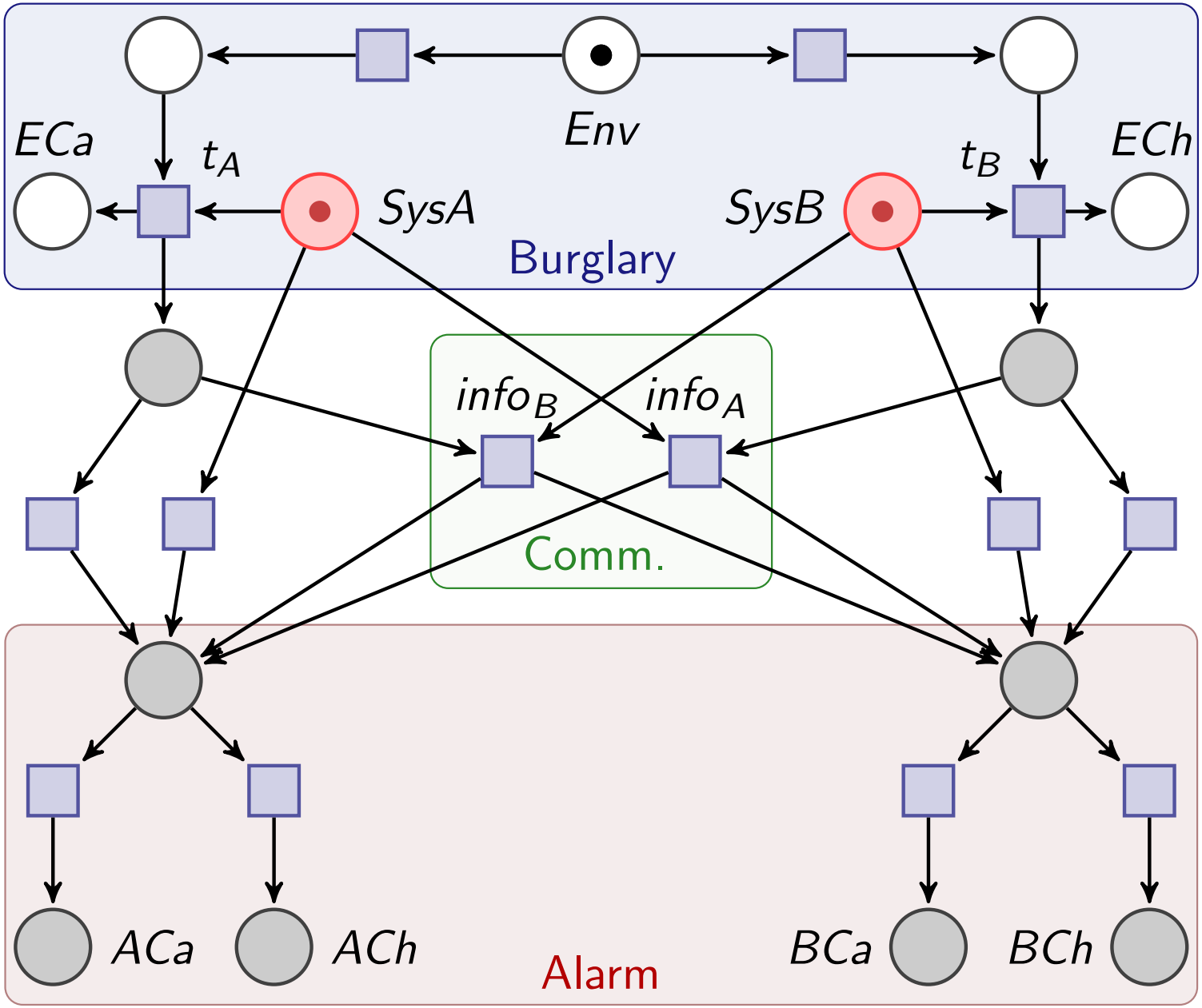
Distributed Alarm Systems



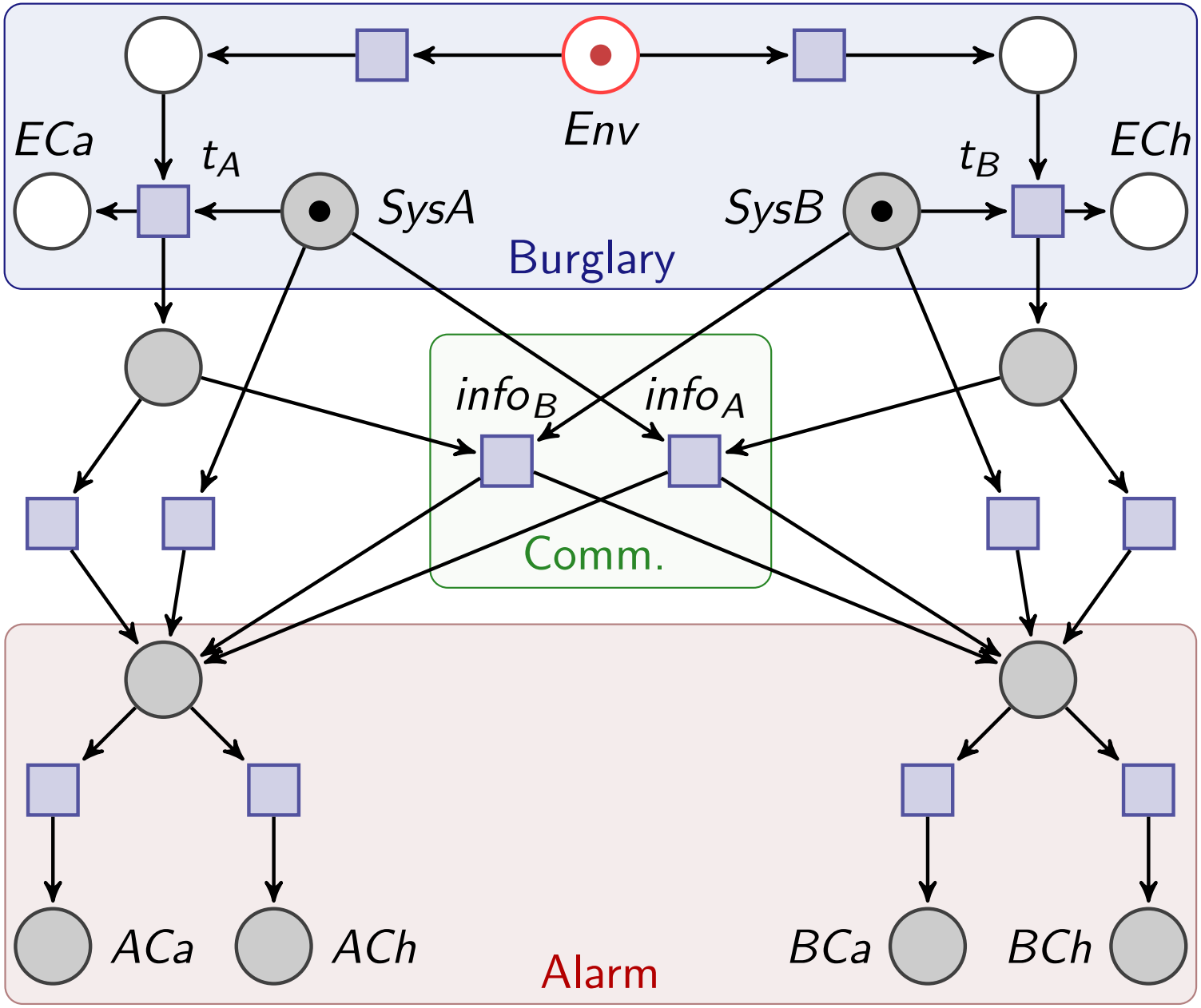
Petri Games are based on Petri Nets



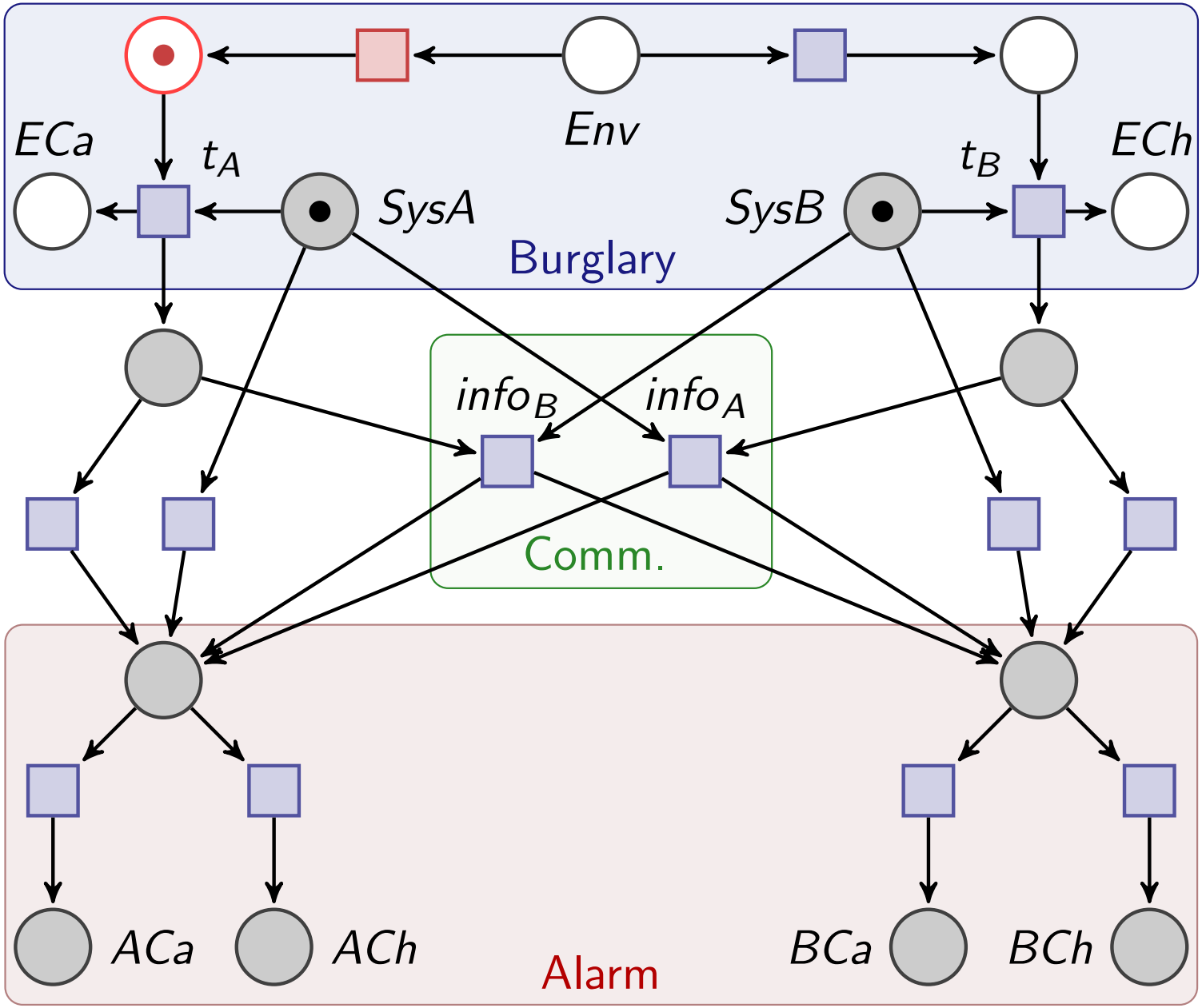
Two System Players



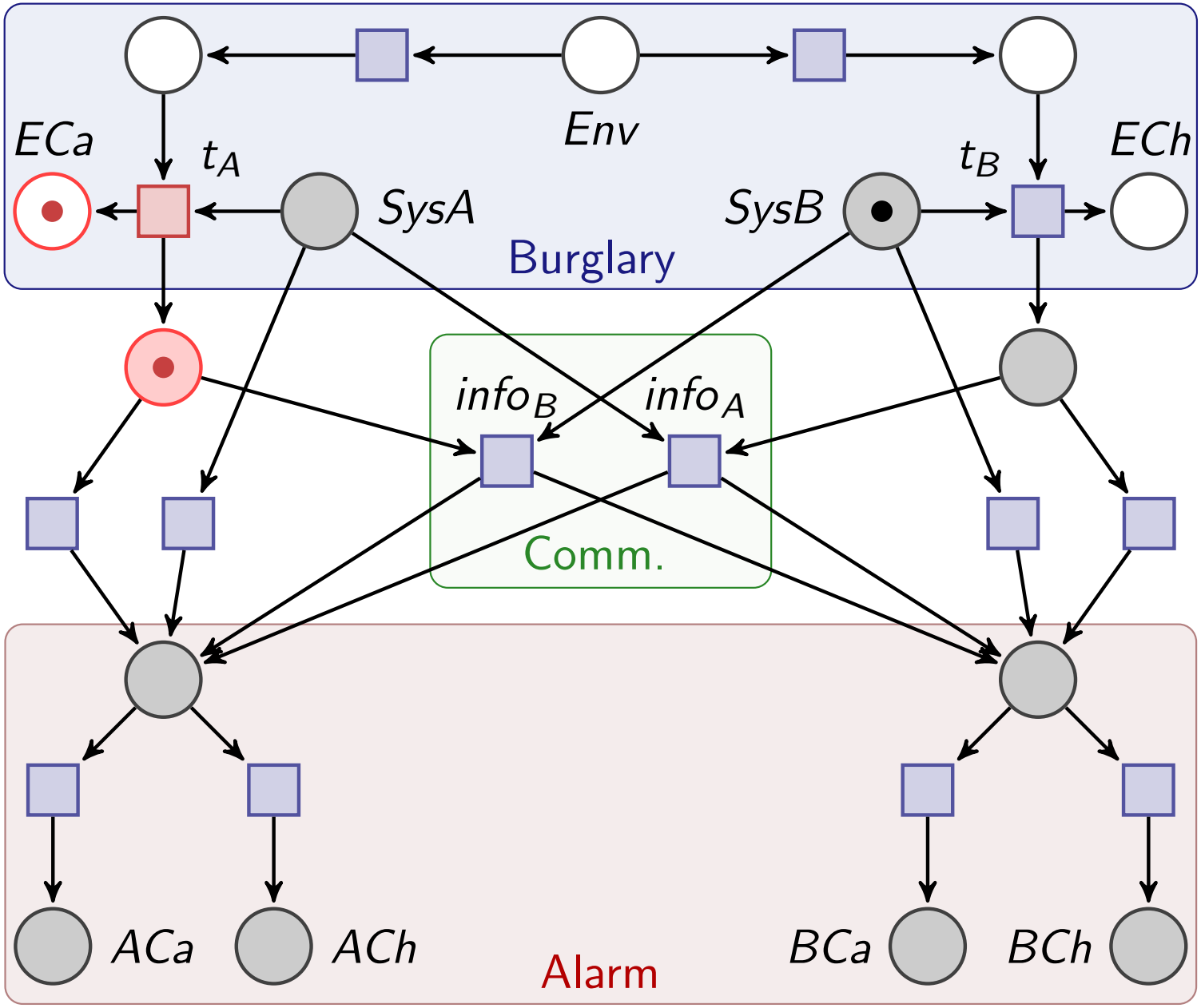
One Environment Player



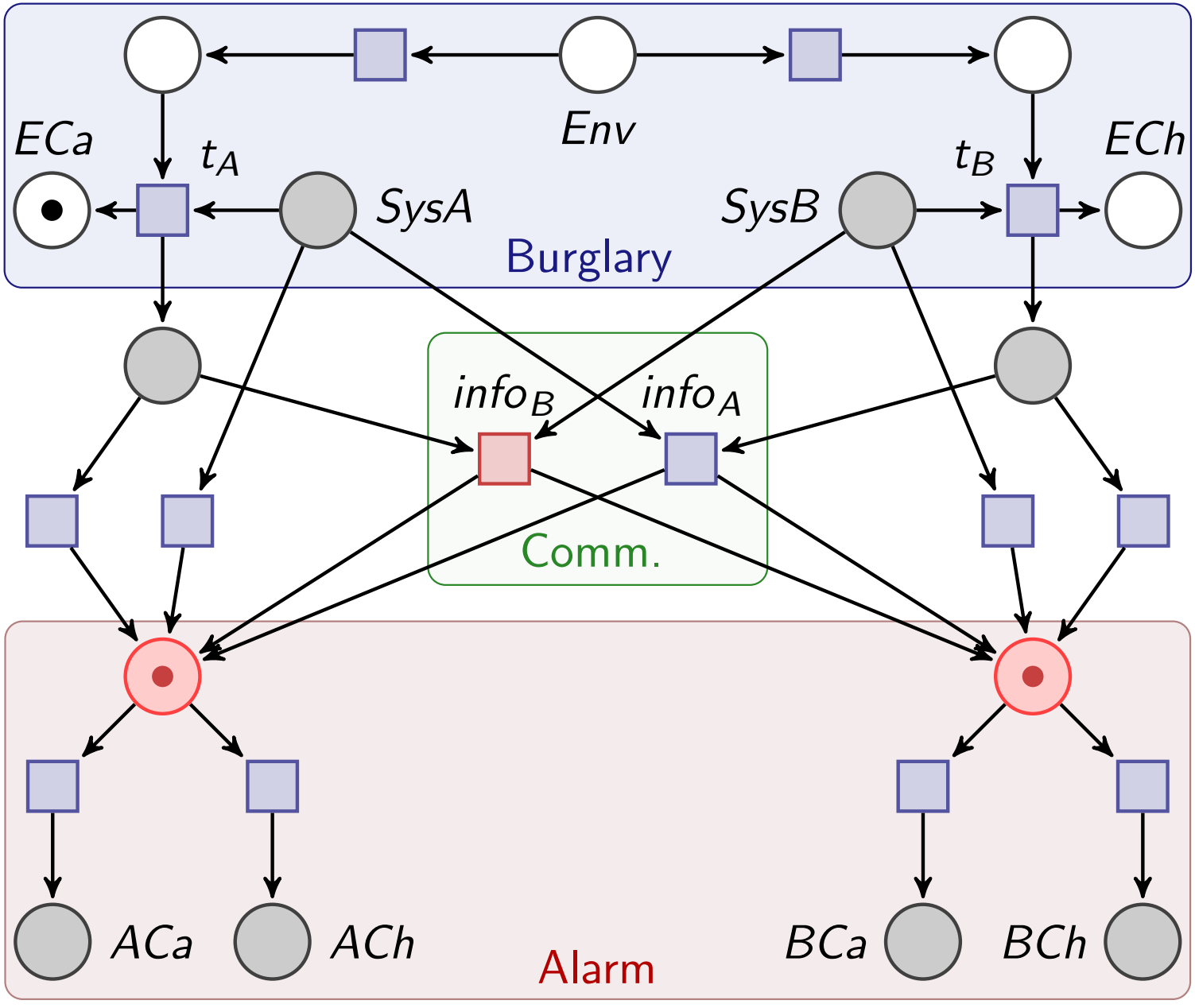
Intrusion at Location A



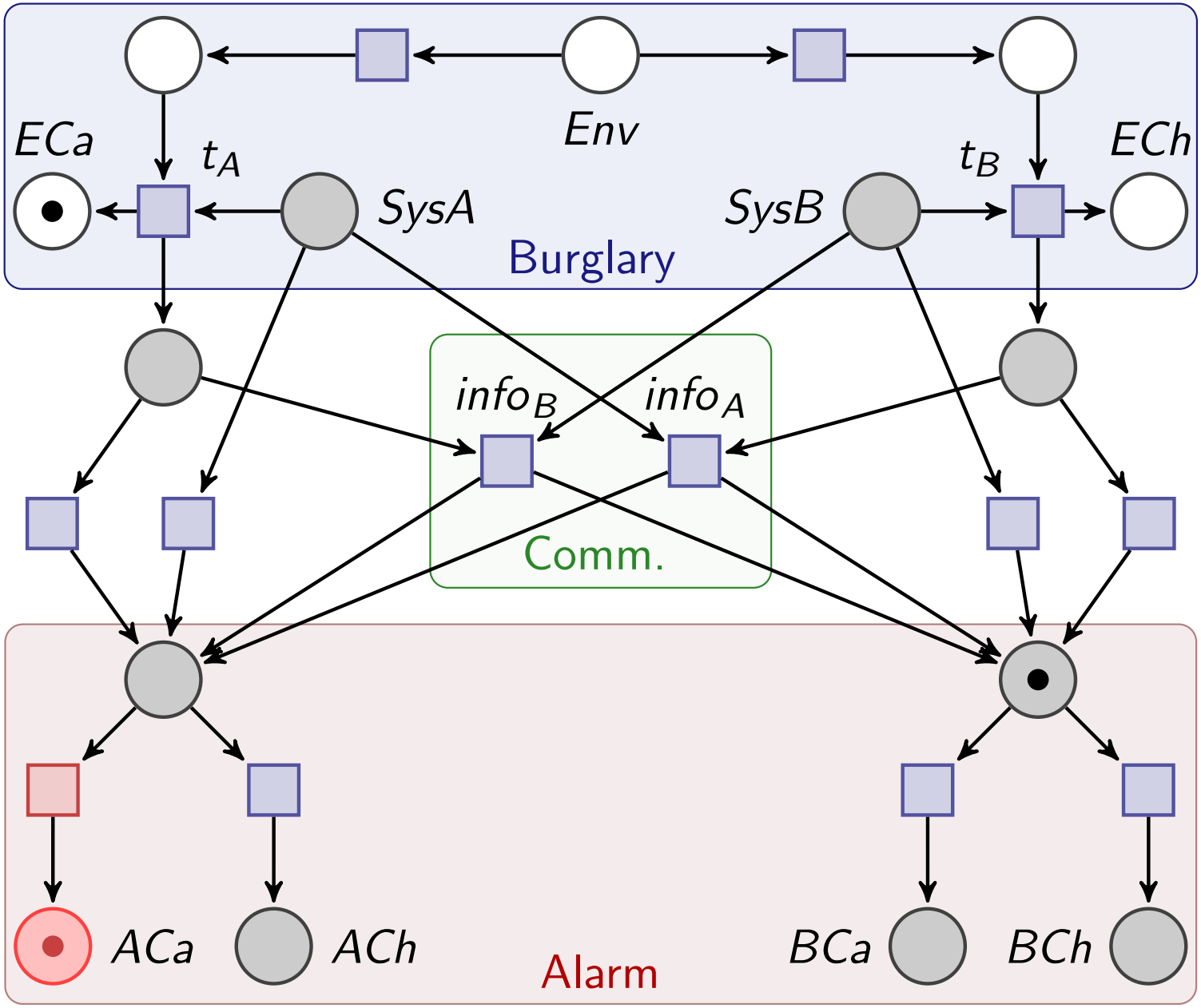
Detection of Intrusion via Synchronization



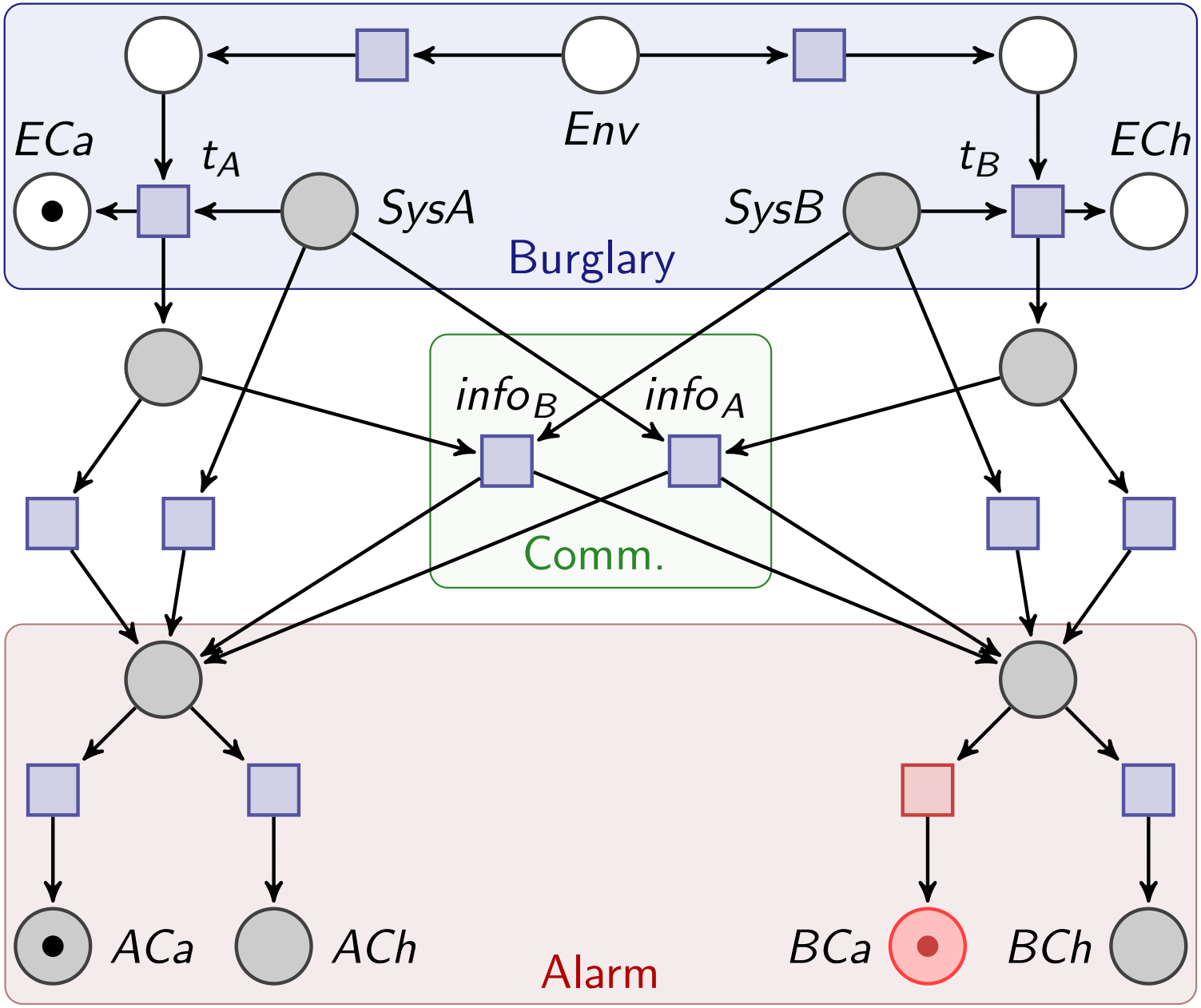
Exchange of Information via Synchronization



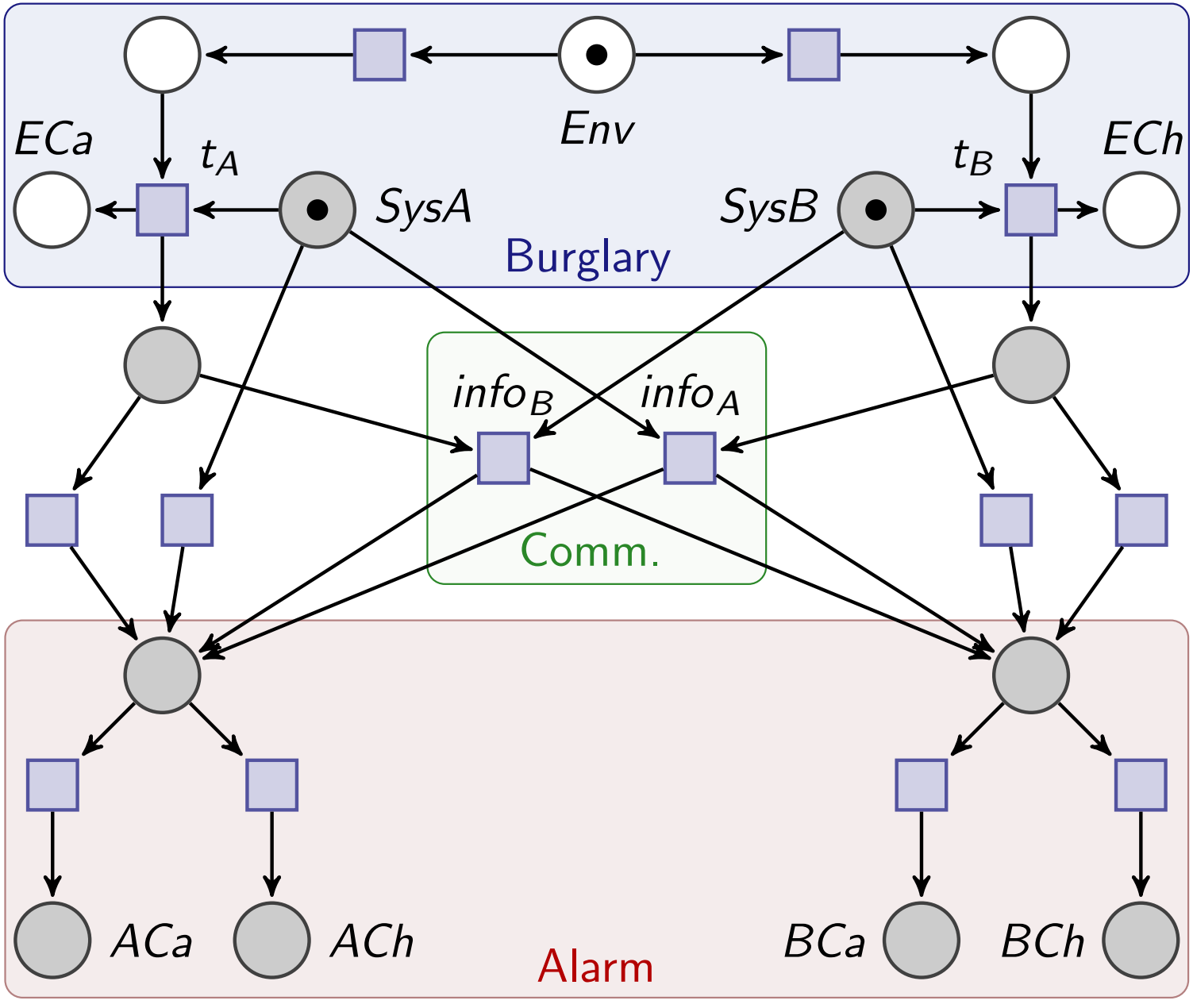
Setting-Off an Alarm



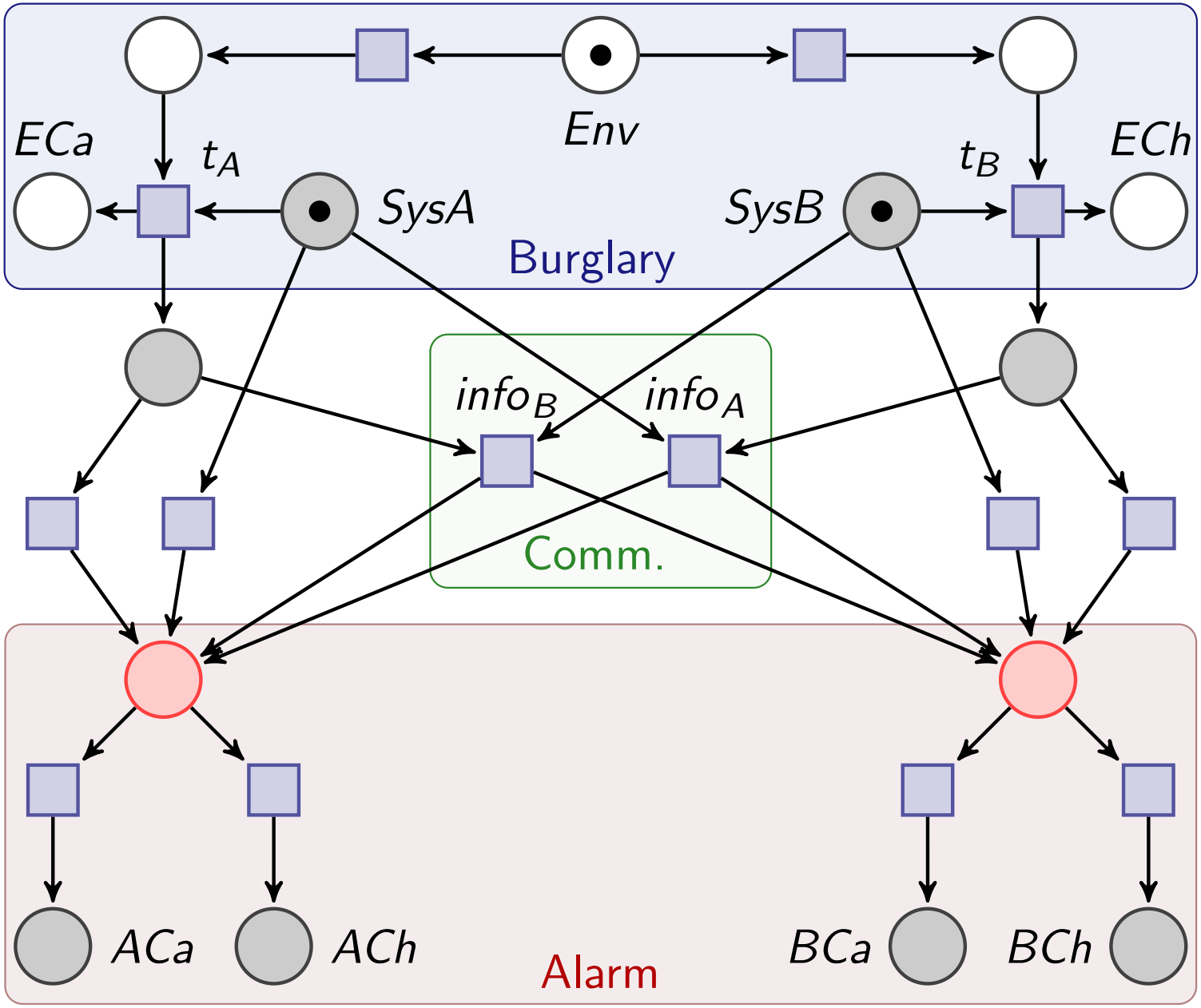
Setting-Off the Second Alarm



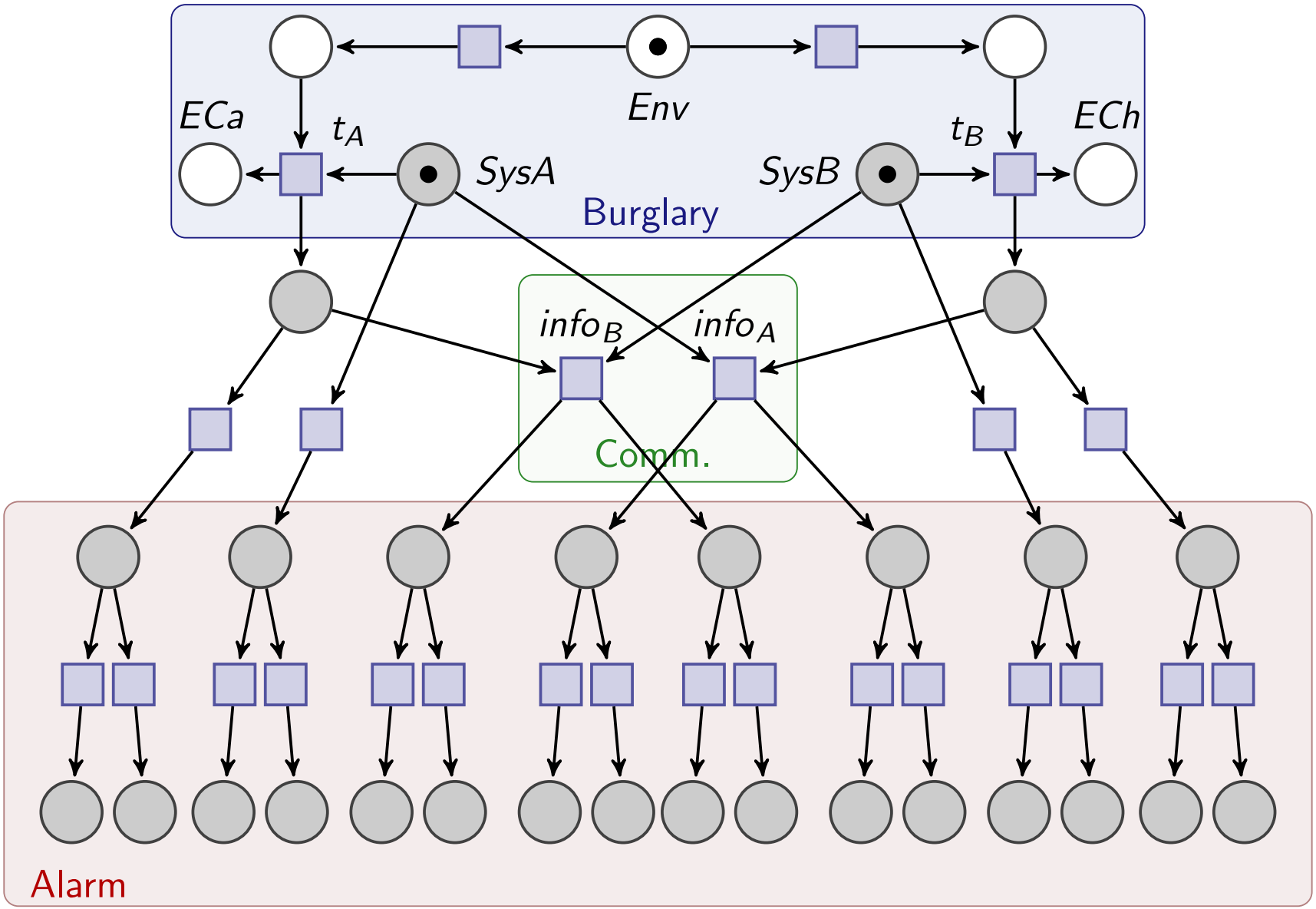
System Players can Refuse to Fire Transitions...



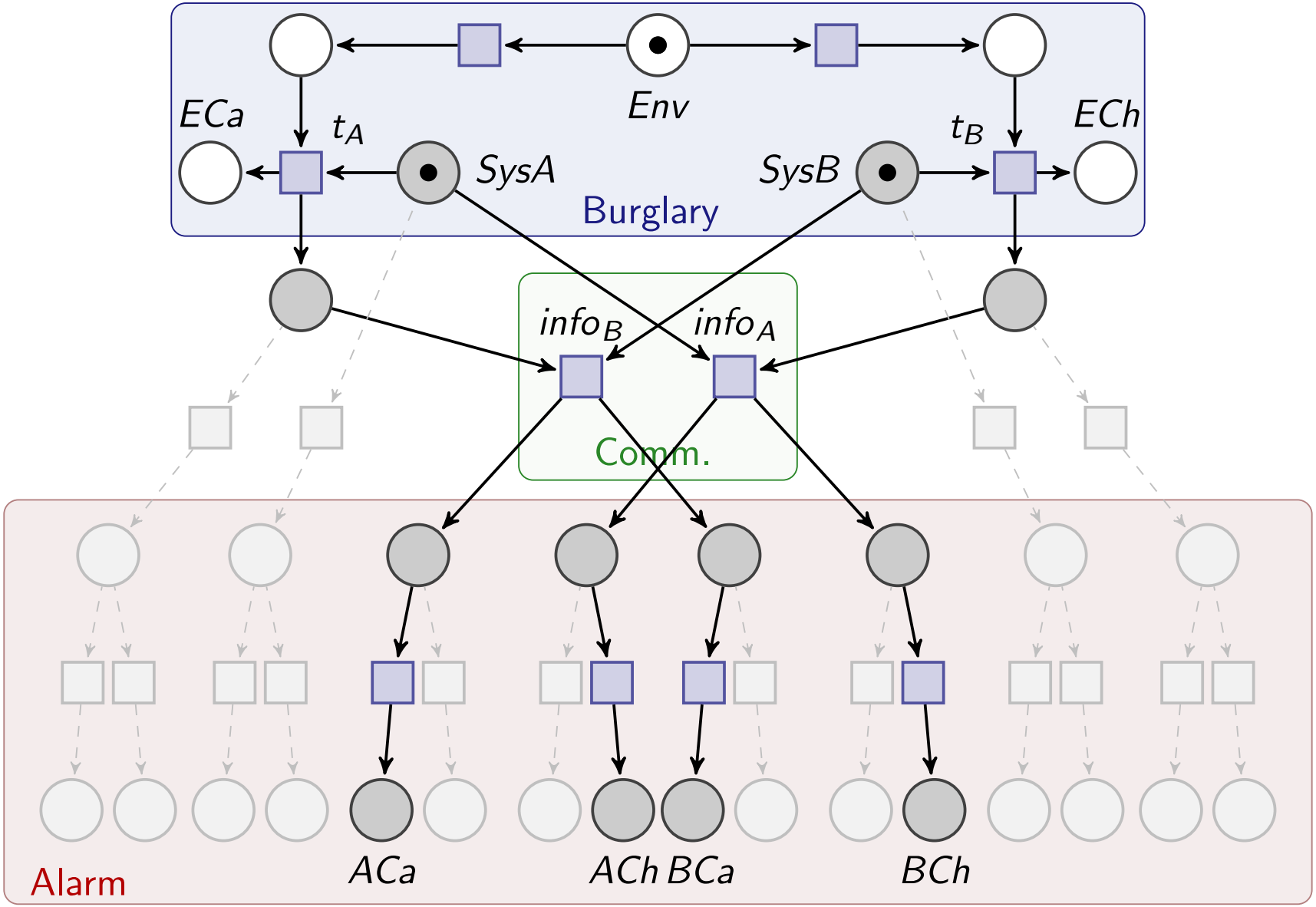
...Based on their Causal Memory



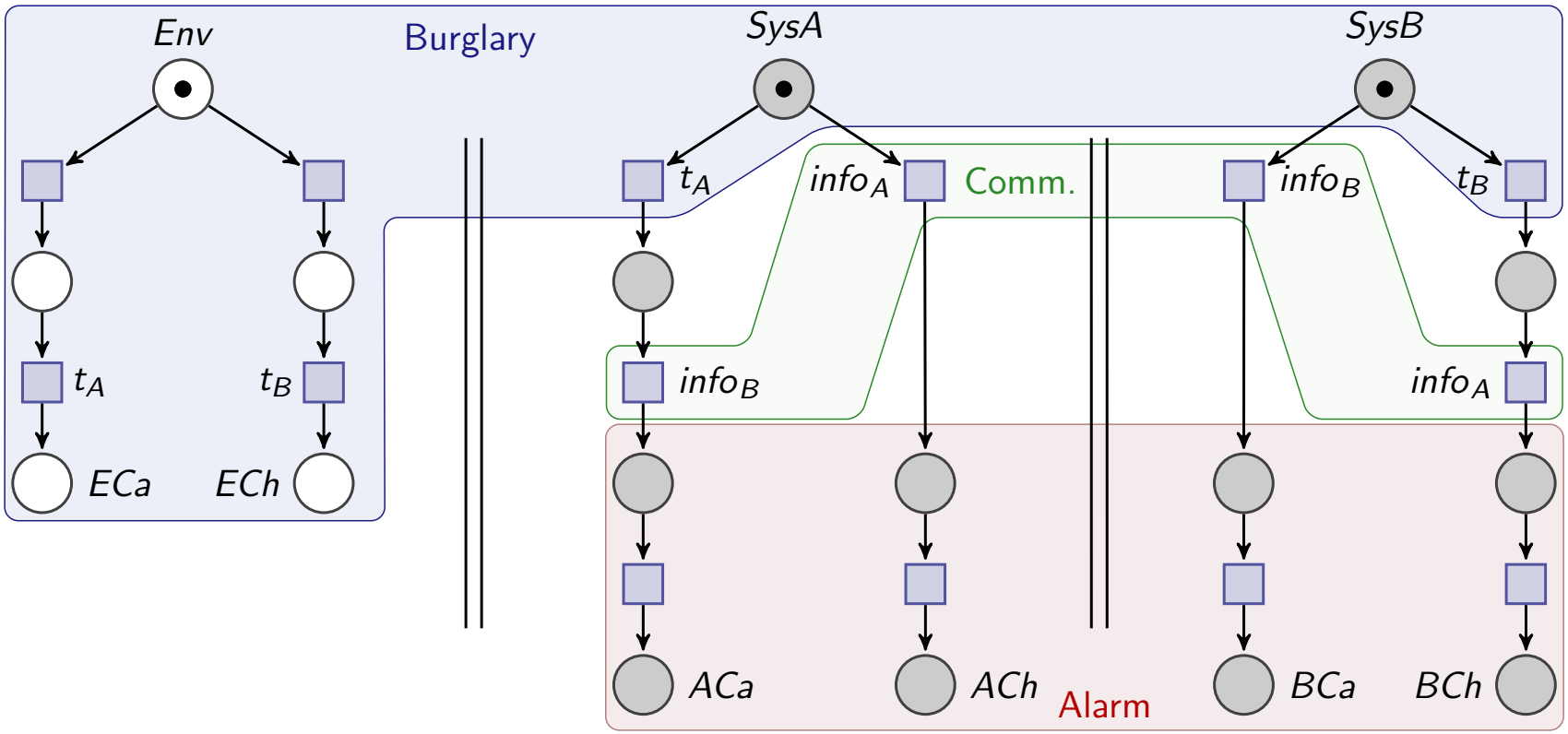
Unfolding of Distributed Alarm System



Winning Strategy of Distributed Alarm System



Local controllers for Distributed Alarm System



Complexity of Solving Petri Games

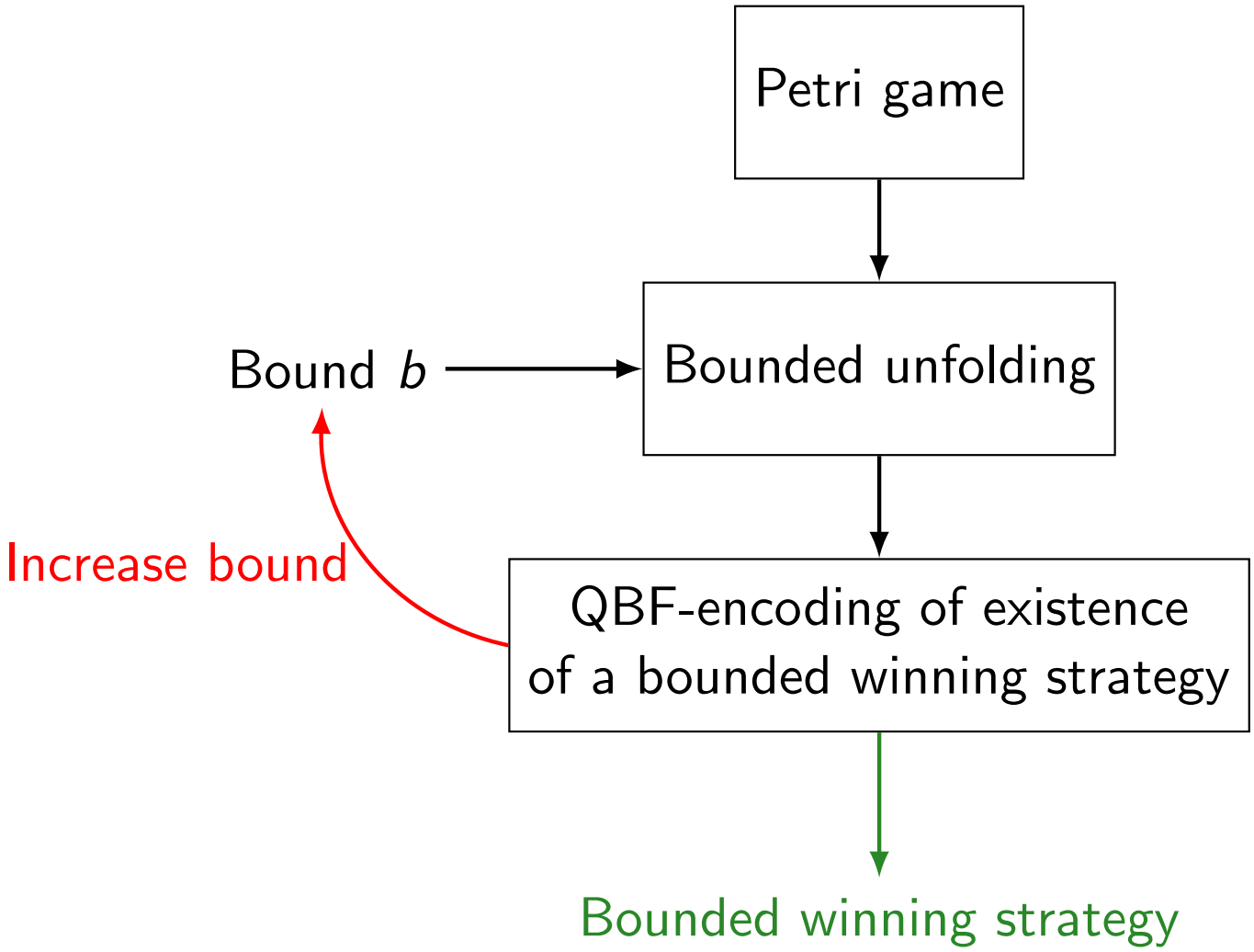
For a single environment token and a bounded number of system tokens, deciding the existence of a safety strategy for the system players is EXPTIME-complete [Finkbeiner, Olderog, '14].

Complexity of Solving Petri Games

For a single environment token and a bounded number of system tokens, deciding the existence of a safety strategy for the system players is EXPTIME-complete [Finkbeiner, Olderog, '14].

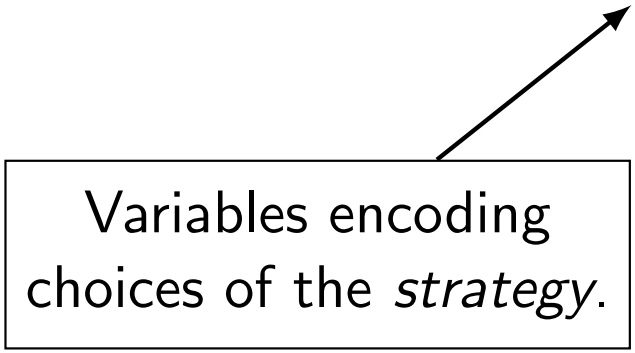
Underlying reduction to a Büchi game implemented in ADAM symbolically [Finkbeiner, Gieseking, Olderog, '15].

Bounded Synthesis for Petri Games

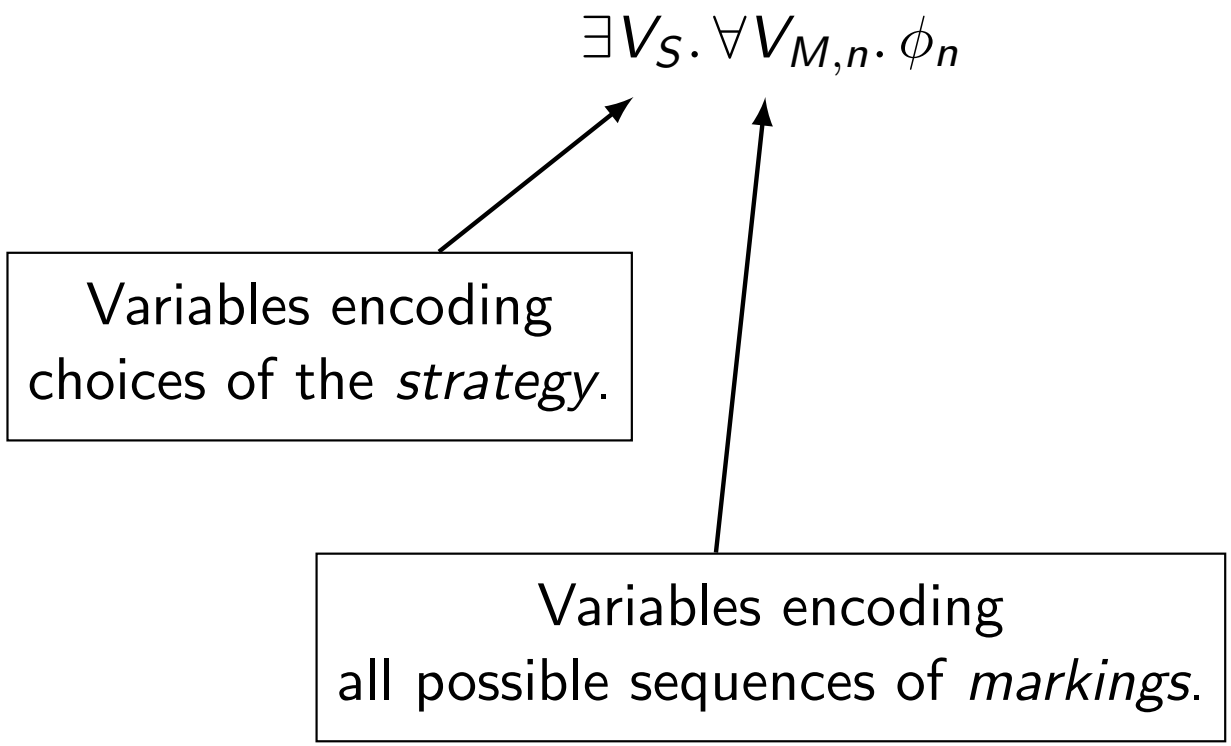


QBF-Encoding of Existence of Bounded Winning Strategy

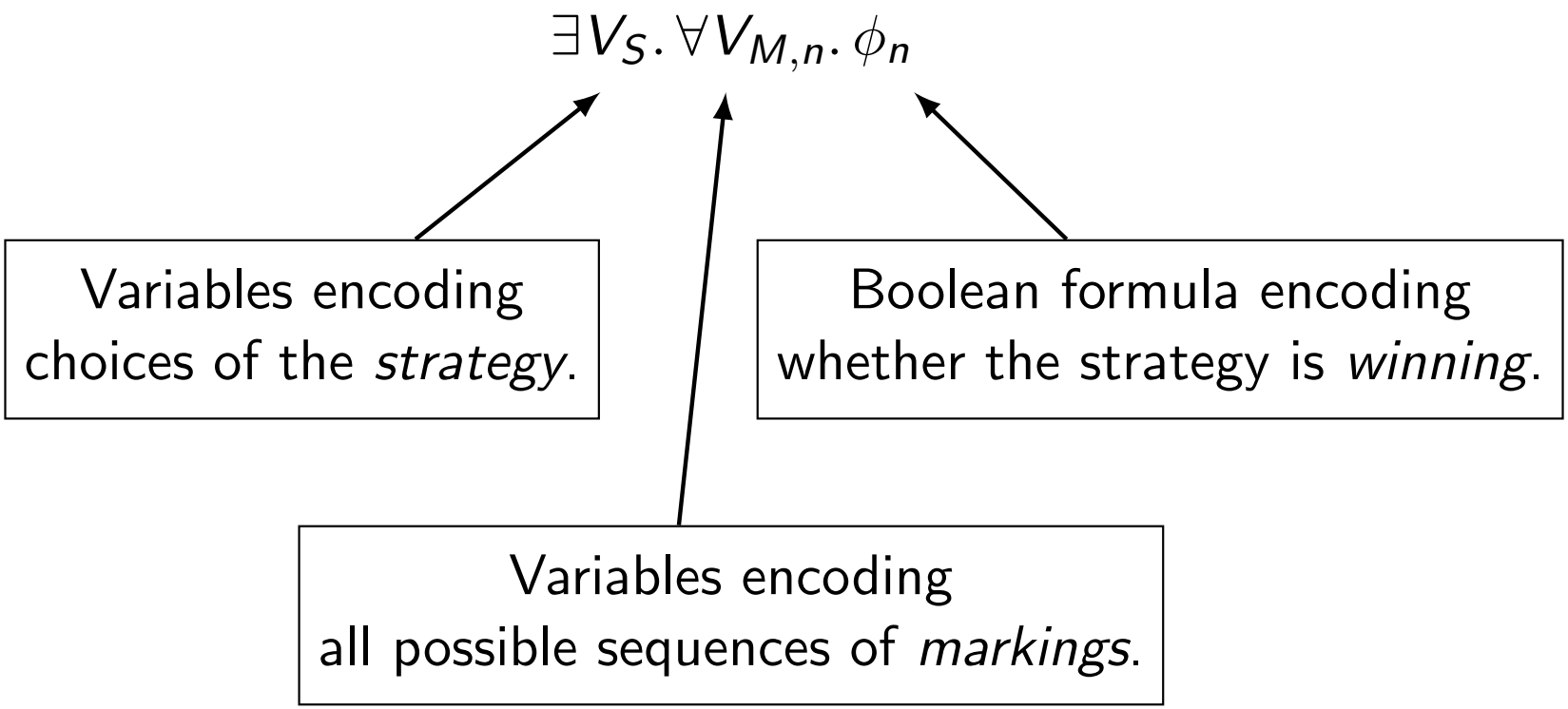
$$\exists V_S . \forall V_{M,n} . \phi_n$$



QBF-Encoding of Existence of Bounded Winning Strategy

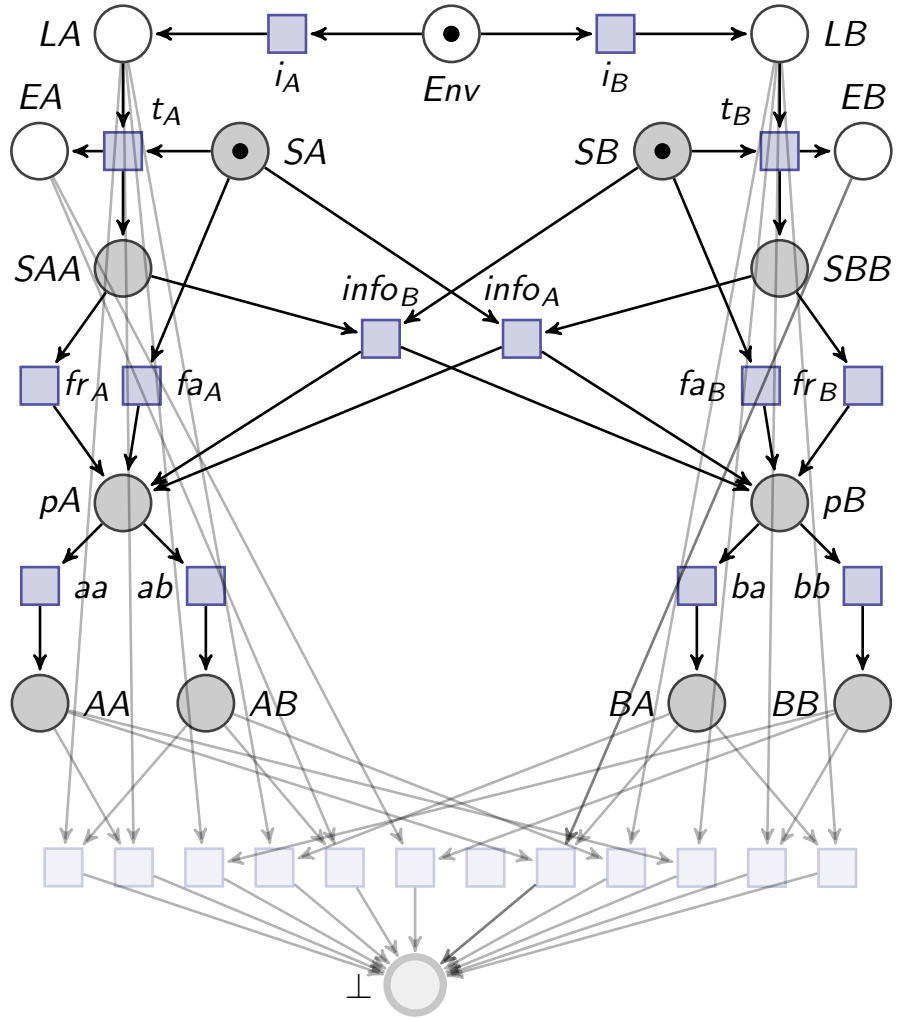


QBF-Encoding of Existence of Bounded Winning Strategy

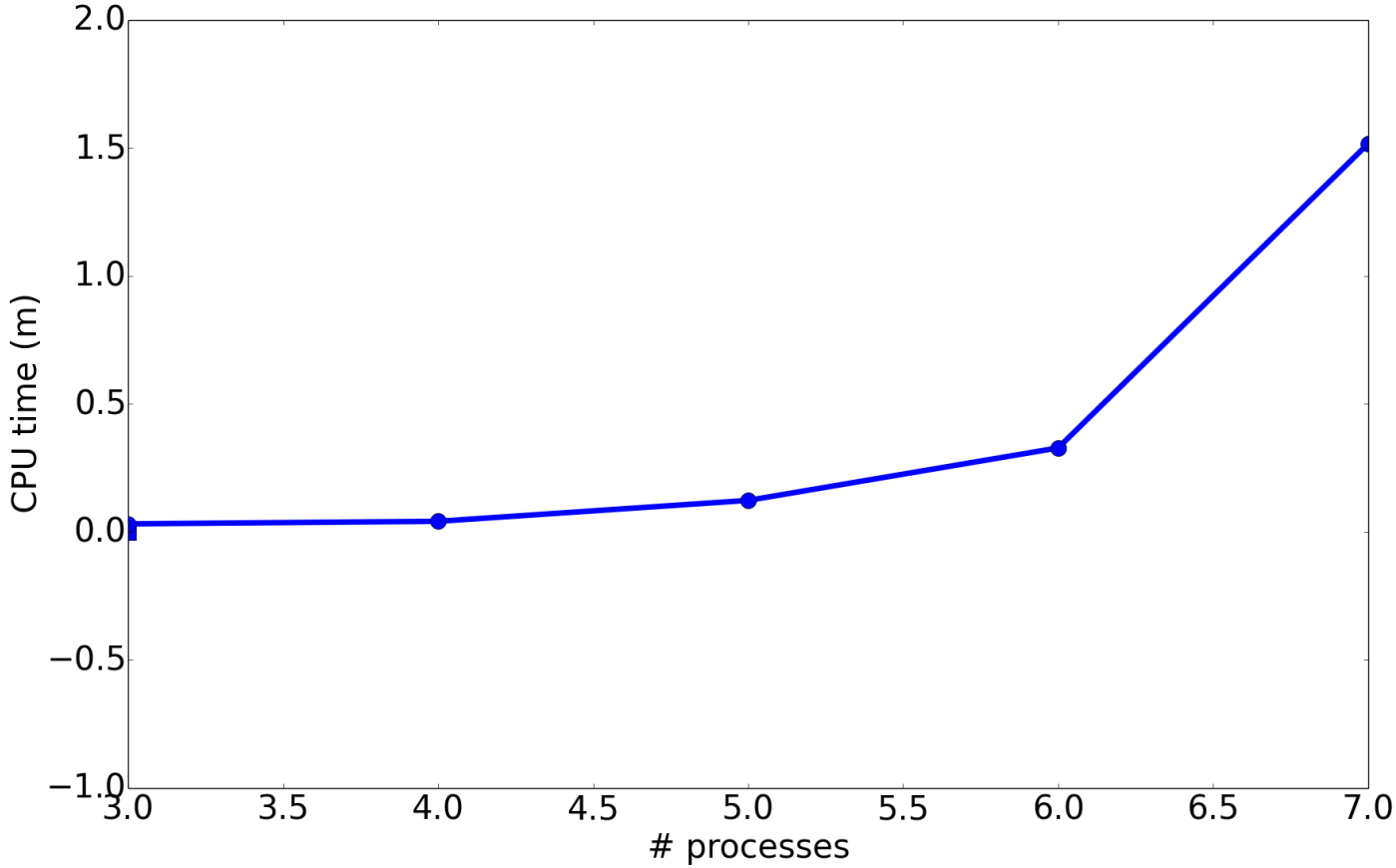


Benchmark – Distributed Alarm System

- The environment can intrude one of n locations.
- All n locations have to indicate where the intrusion occurred.
- Scalable in n



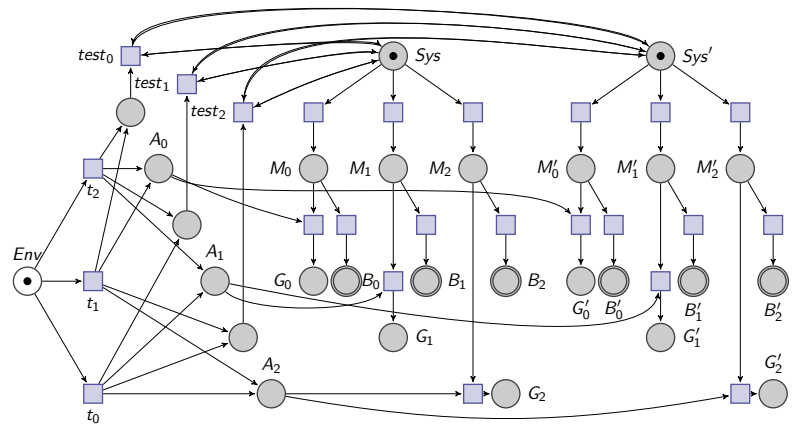
Runtime – Distributed Alarm System



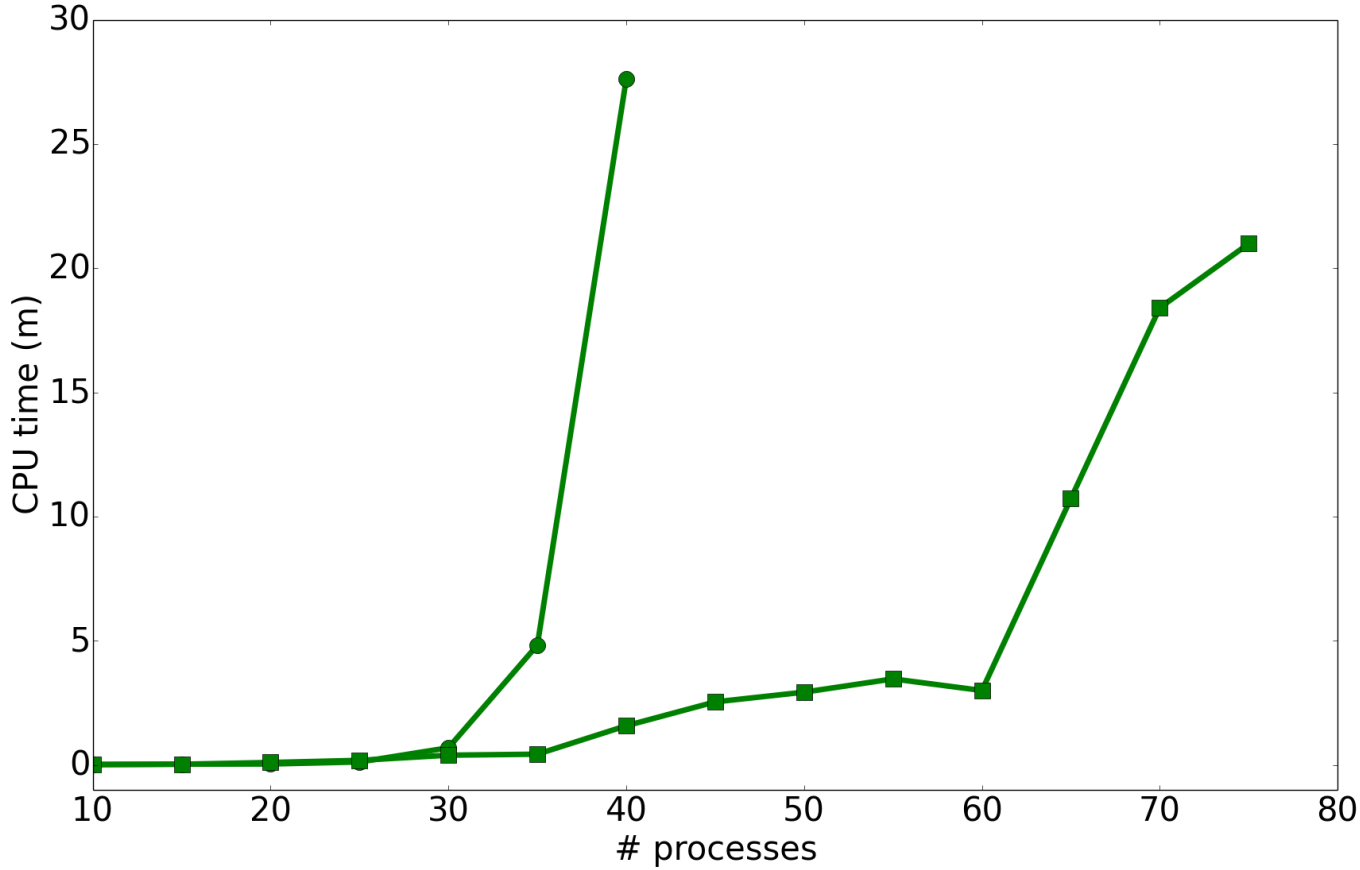
- winning strategy of symbolic approach,
- winning strategy of bounded approach

Benchmark – Concurrent Machines

- k orders to manufacture goods are processed by n distributed machines.
- The environment can destroy one machine.
- The orders have to avoid the defective machines and each machine can process at most one order.
- Scalable in n and k



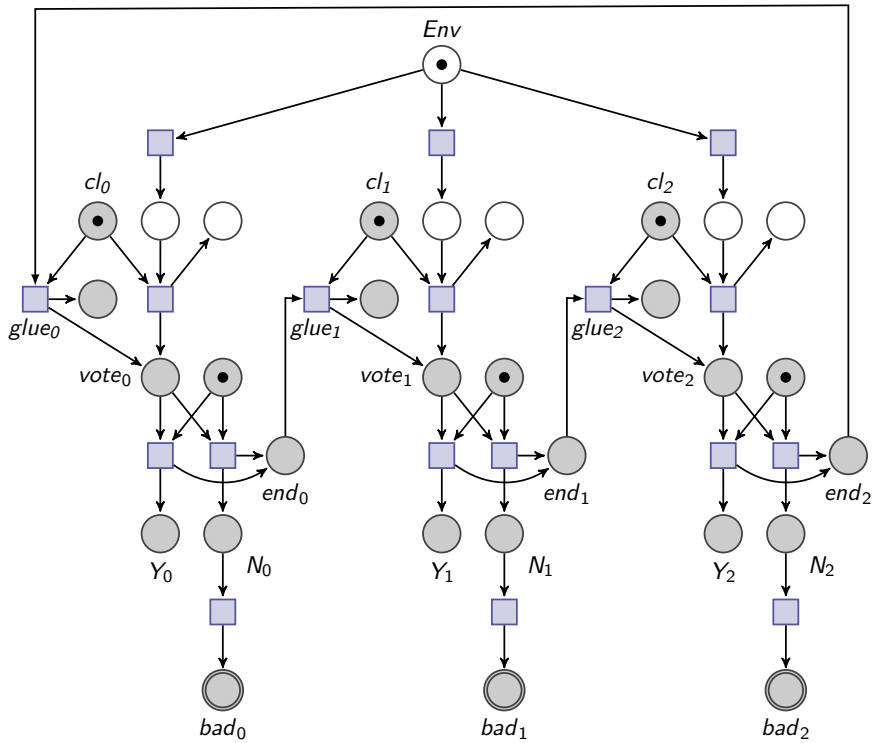
Runtime – Concurrent Machines



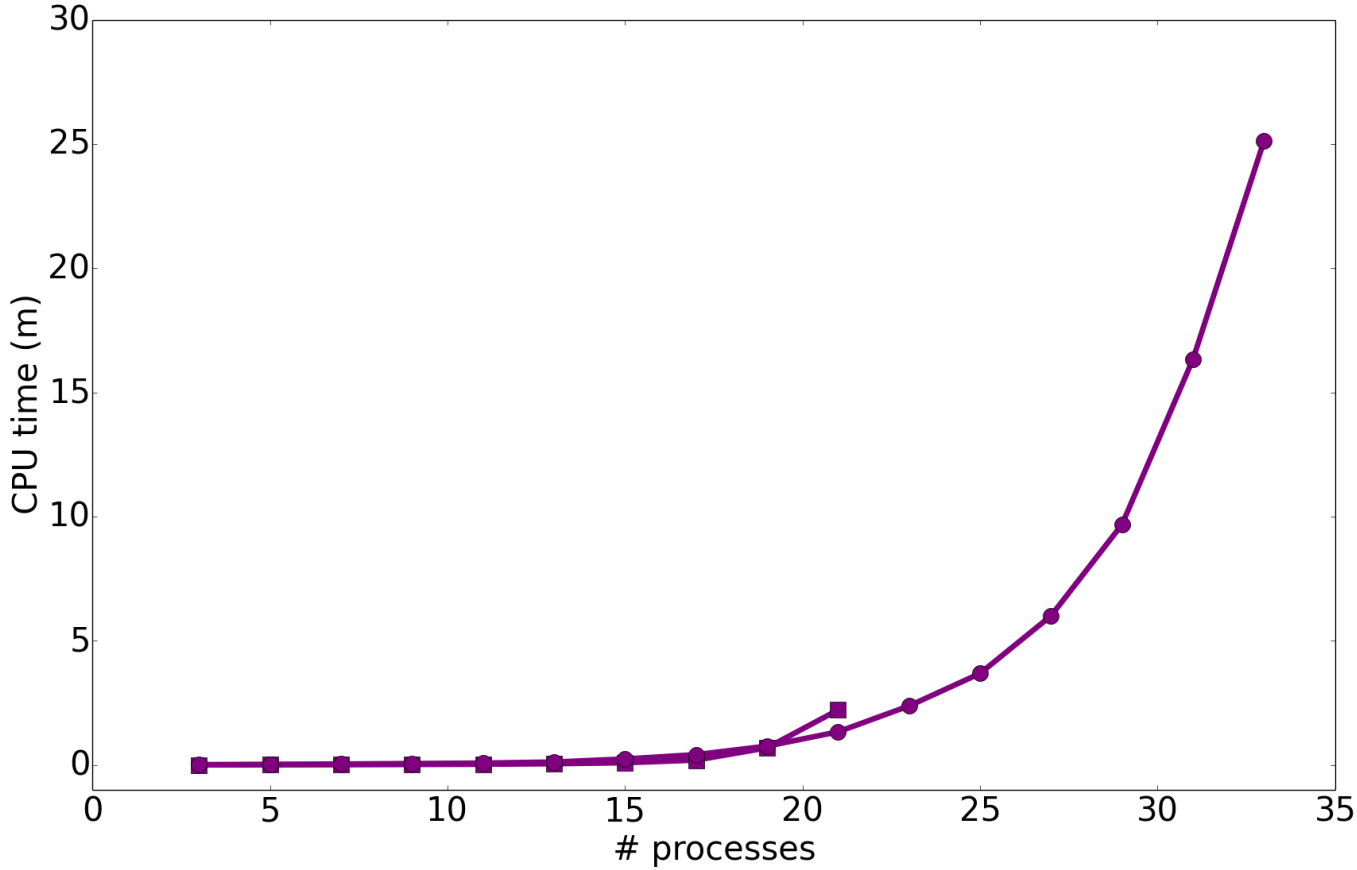
- winning strategy of symbolic approach,
- winning strategy of bounded approach

Benchmark – Document Workflow simple

- n clerks should endorse a document.
- The environment decides which clerk gets the document first.
- scalable in n



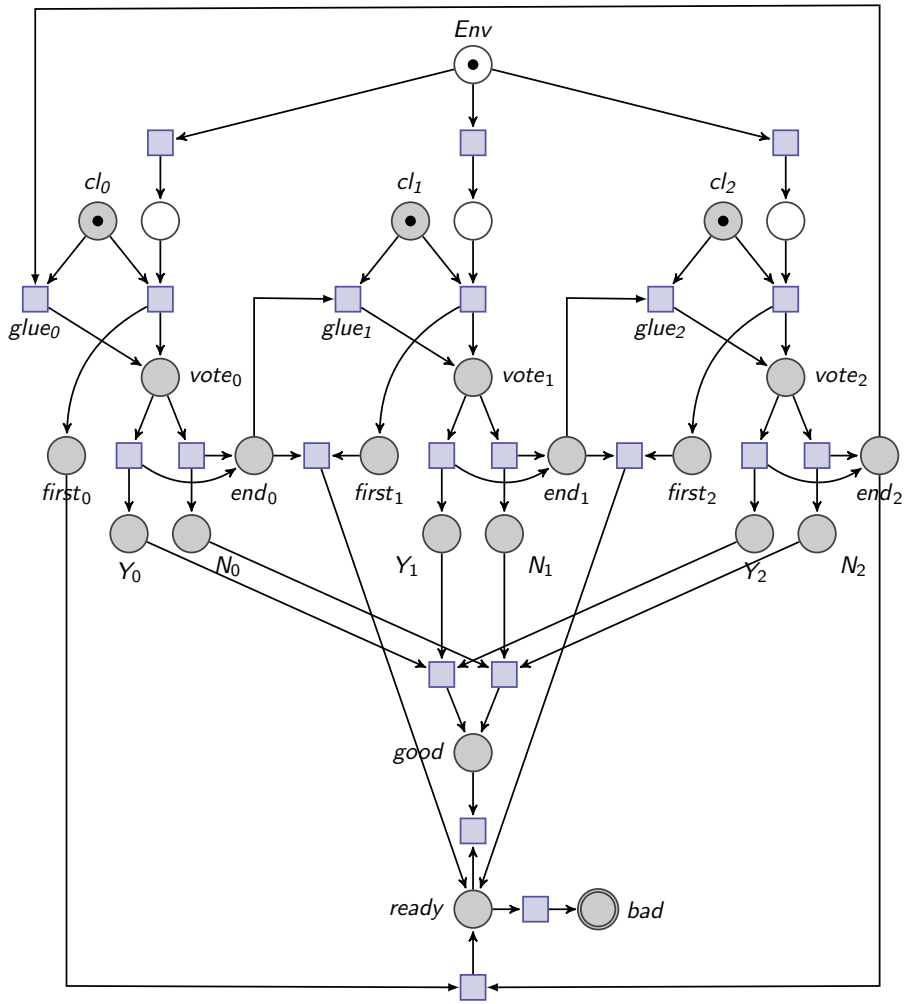
Runtime – Document Workflow simple



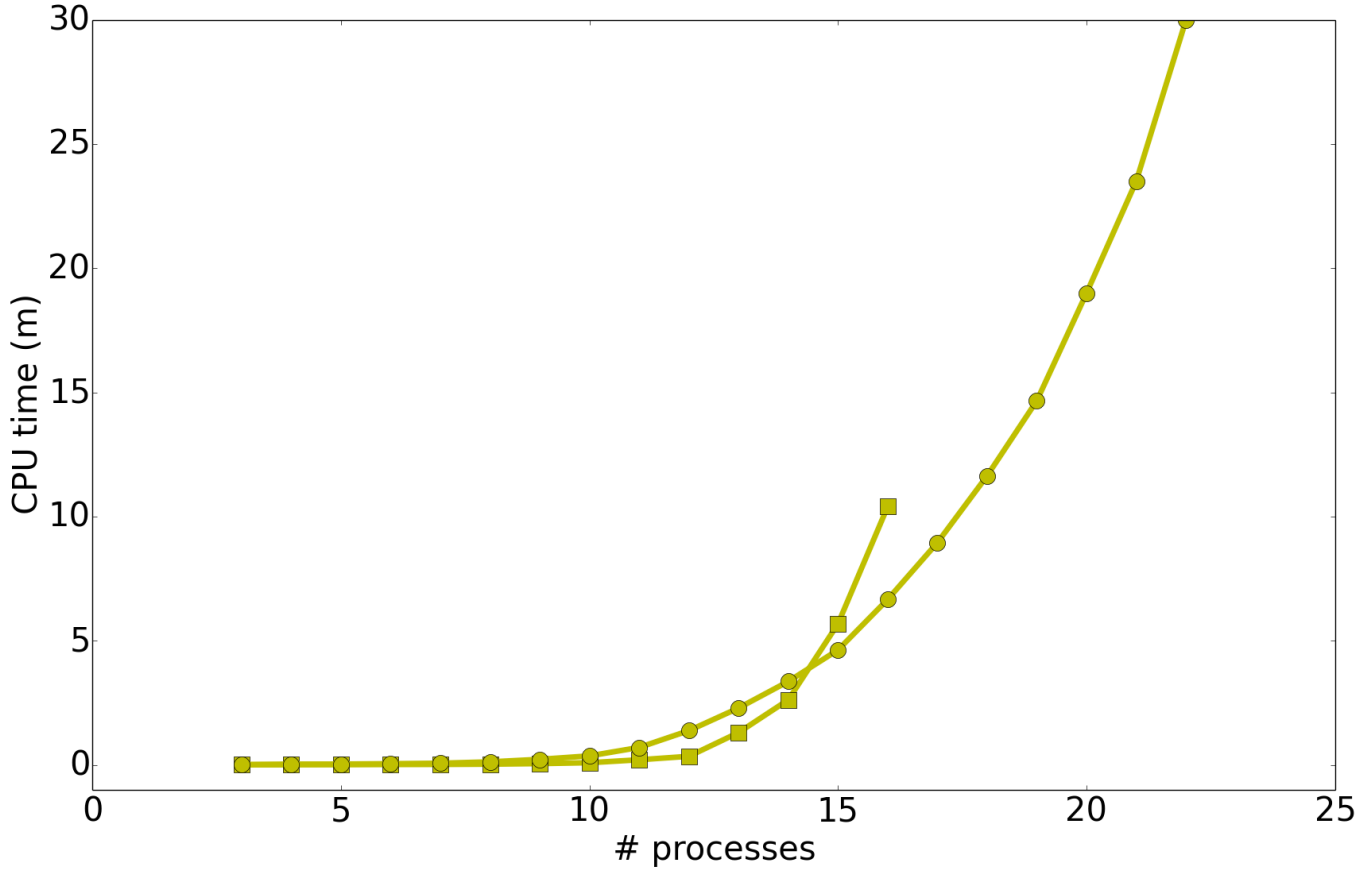
- winning strategy of symbolic approach,
- winning strategy of bounded approach

Benchmark – Document Workflow

- n clerks have to make a unanimous decision to endorse or reject the document.
- The environment decides which clerk has to start.
- scalable in n



Runtime – Document Workflow

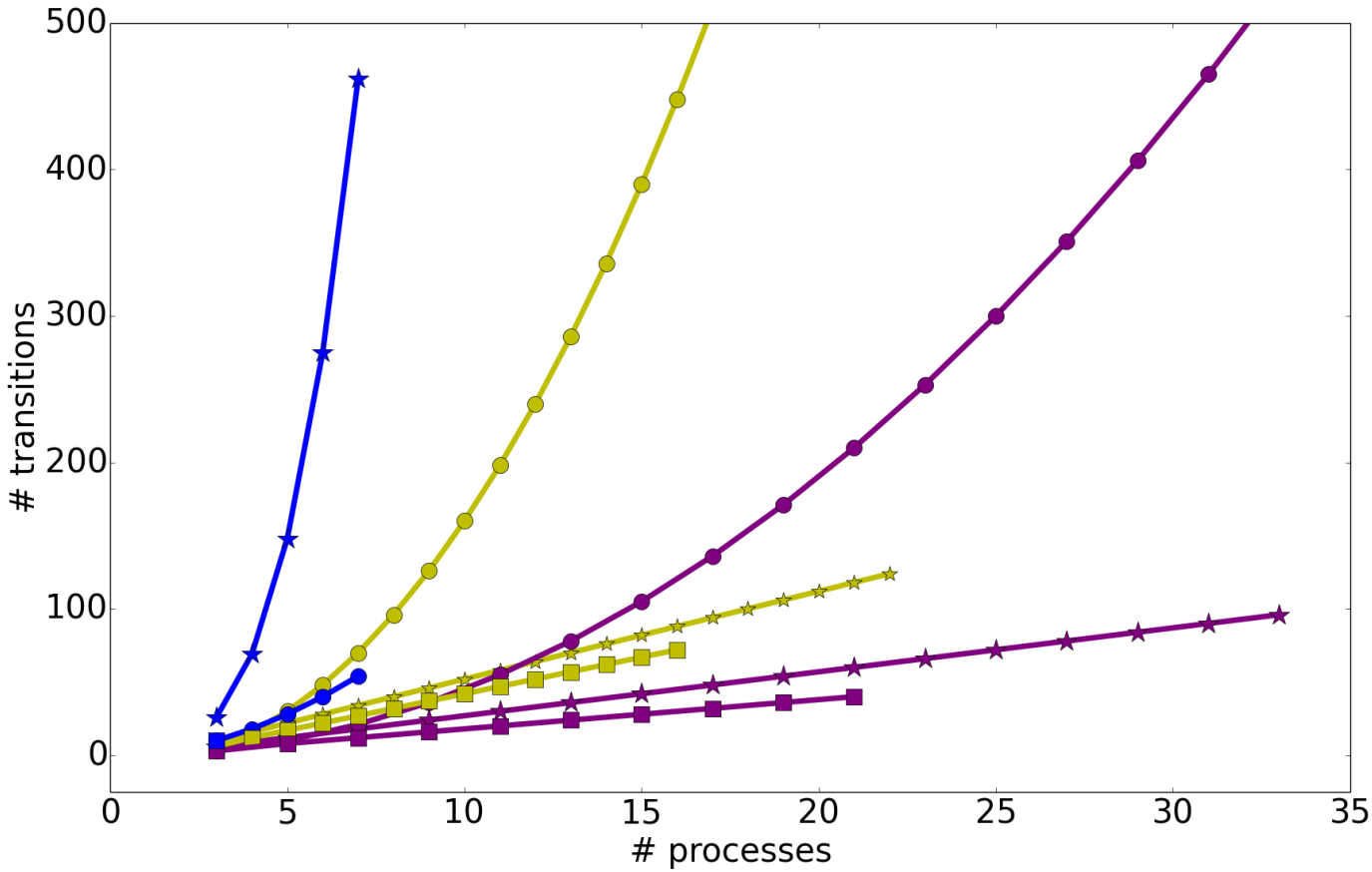


- winning strategy of symbolic approach,
- winning strategy of bounded approach

Results for Comparison of Runtime

- The symbolic approach has better runtime for benchmarks with numerous transitions to bad places.
- The bounded approach synthesizes distributed systems with up to 75 processes.

Strategy Size of Symbolic and Bounded Approach



- ⋆ input Petri game
- • winning strategy of symbolic approach
- ■ bounded winning strategy

Results for Comparison of Strategy Size

- The bounded unfolding allows succinct representation of situations where the same decision suffices for different causal pasts.

Conclusions

- Petri games are the first scalable framework for distributed synthesis of systems with up to 75 distributed components.
- Winning strategies of the bounded approach are by order of magnitude smaller than winning strategies of the symbolic approach.
- Bounded synthesis solves games with more than one environment player which we plan to realize for the symbolic approach in future work (including further benchmarks).