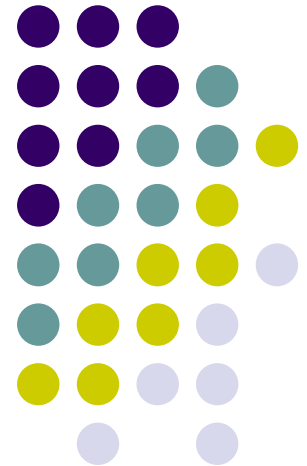


Formal Behavioural Models and Compliance Analysis for Service Oriented Systems



Natallia Kokash
and
Farhad Arbab





Introduction



- Role of Formal Methods in SOA
- COMPAS Project
- Reo Coordination Language
- From Business Process Modeling (BPM) to Web Service (WS) Composition
 - BPMN to Reo mapping
 - Process analysis, examples
- Support for Business Process Compliance
 - Control flow, transactions, temporal requirements, Quality of Service (QoS)
- Conclusions and Future Work

Role of Formal Methods in SOC



- Analysis of composition/coordination languages (e.g., WS-BPEL, WS-CDL)
- Complete unambiguous description of service behavior and non-functional properties
- Verification of service interaction protocols
- Analysis of WS compositions (behavioral compatibility of services, performance analysis, security, etc.)
- Support for automated WS composition
- ...



COMPAS project



- COMPAS = Compliance-driven Models, Languages, and Architectures for Services
 - *Ensure dynamic and on-going compliance of software services to business regulations and user requirements*
 - *Help organizations to develop business compliance solutions easier and faster*
 - <http://www.compas-ict.eu/>

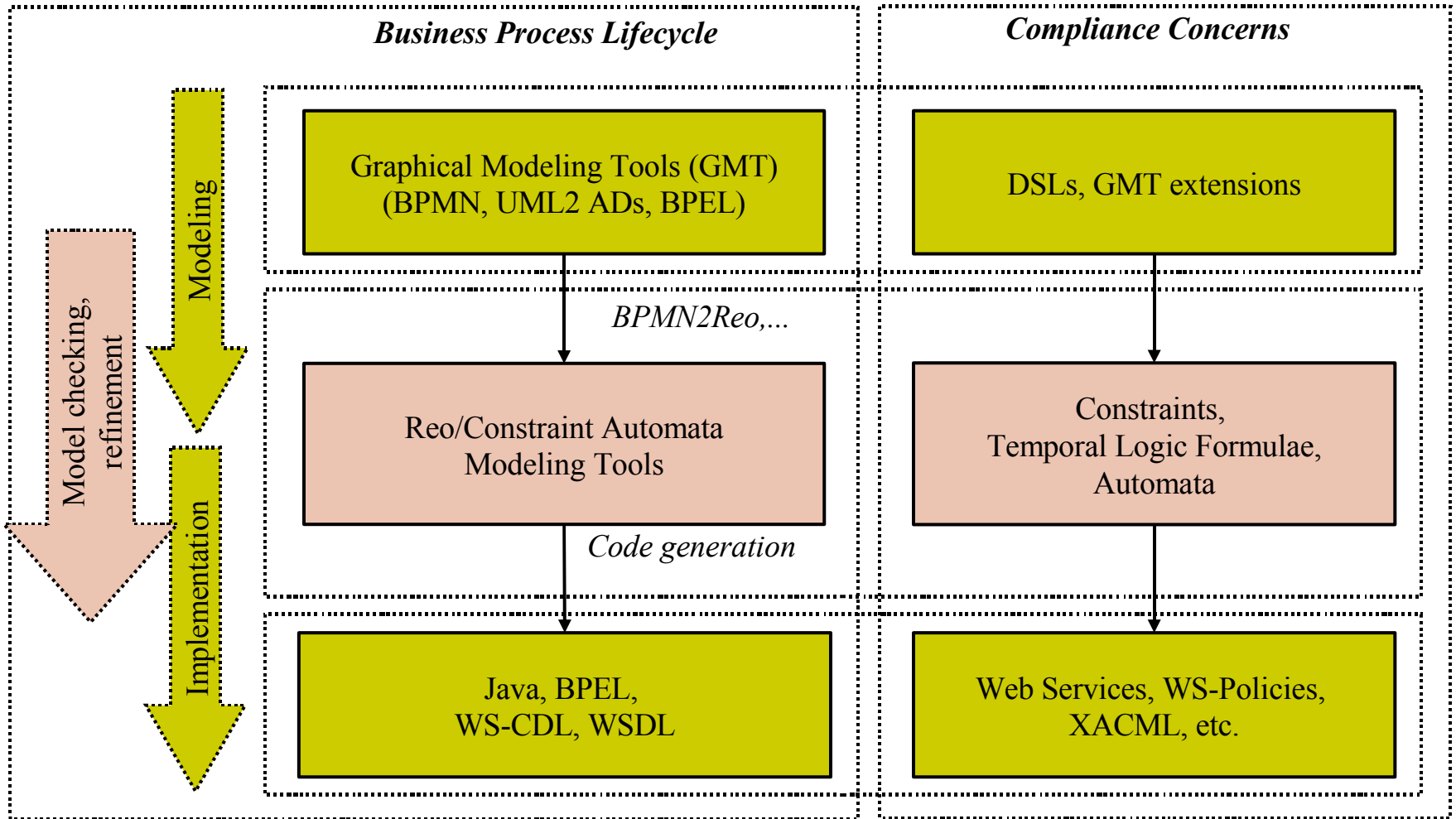
What is Compliance?



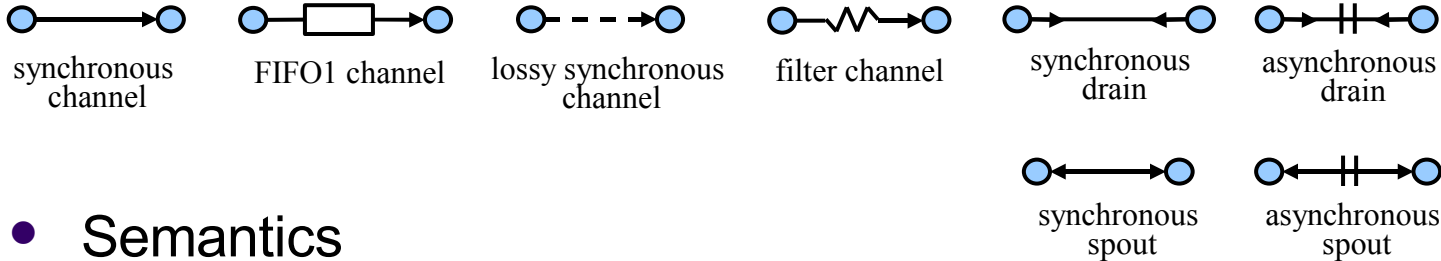
- A multi-faceted concept that encompasses the capability of an organization to meet requirements coming from
 - Regulatory/legislative documents
 - Basel II², Sarbanes-Oxley⁶, IFRS², MiFID³, LSF⁴, HIPAA, Tabaksblat⁵, etc.
 - Internal movements towards Quality of Service (QoS)
 - User-defined constraints...
- Compliance can be seen as
 - A **state** of “adherence of one set of rules (source rules) against another set of rules (target rules)”
 - A **process**, which is about “ensuring that **business processes**, operations and practice are in accordance with a prescribed set of norms”



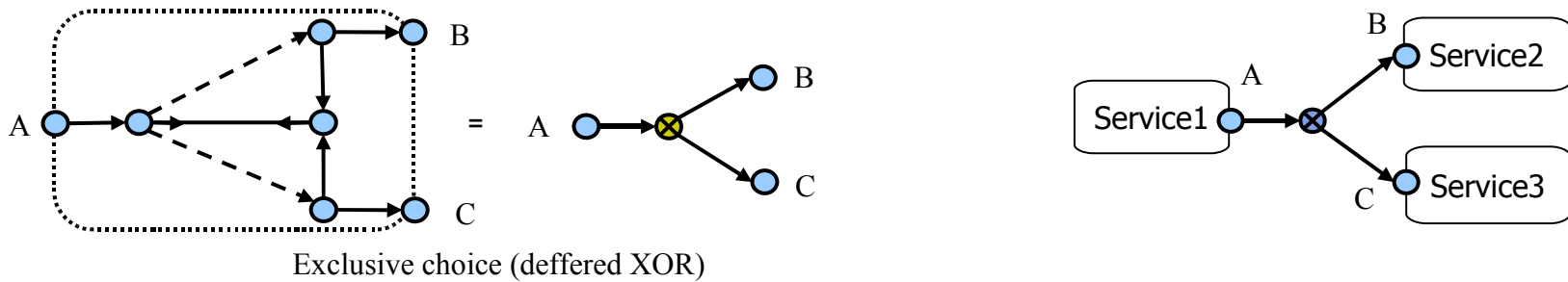
Compliance-aware SOA design



Reo Coordination Language



- Semantics
 - Connector coloring
 - Constraint automata
 - [Baier et al. 2006]





Reo Coordination Tools



- Reo Connector Editor
- Animation Plug-in
- Reconfiguration Plug-in
- Converter to Extended Constraint Automata (time, QoS)
- Model Checking Tool (provided by University of Dresden)
 - http://wwwtcs.inf.tu-dresden.de/~klueppel/TUD_CWI/Welcome
- Java Code Generator (distributed version is also available)
- <http://reo.project.cwi.nl/>

- BPEL to Reo converter (provided by University of Tehran)
 - [S. Tasharofi et al. 2008]
- UML Sequence Diagrams to Reo converter – work in progress
- BPMN to Reo converter – work in progress

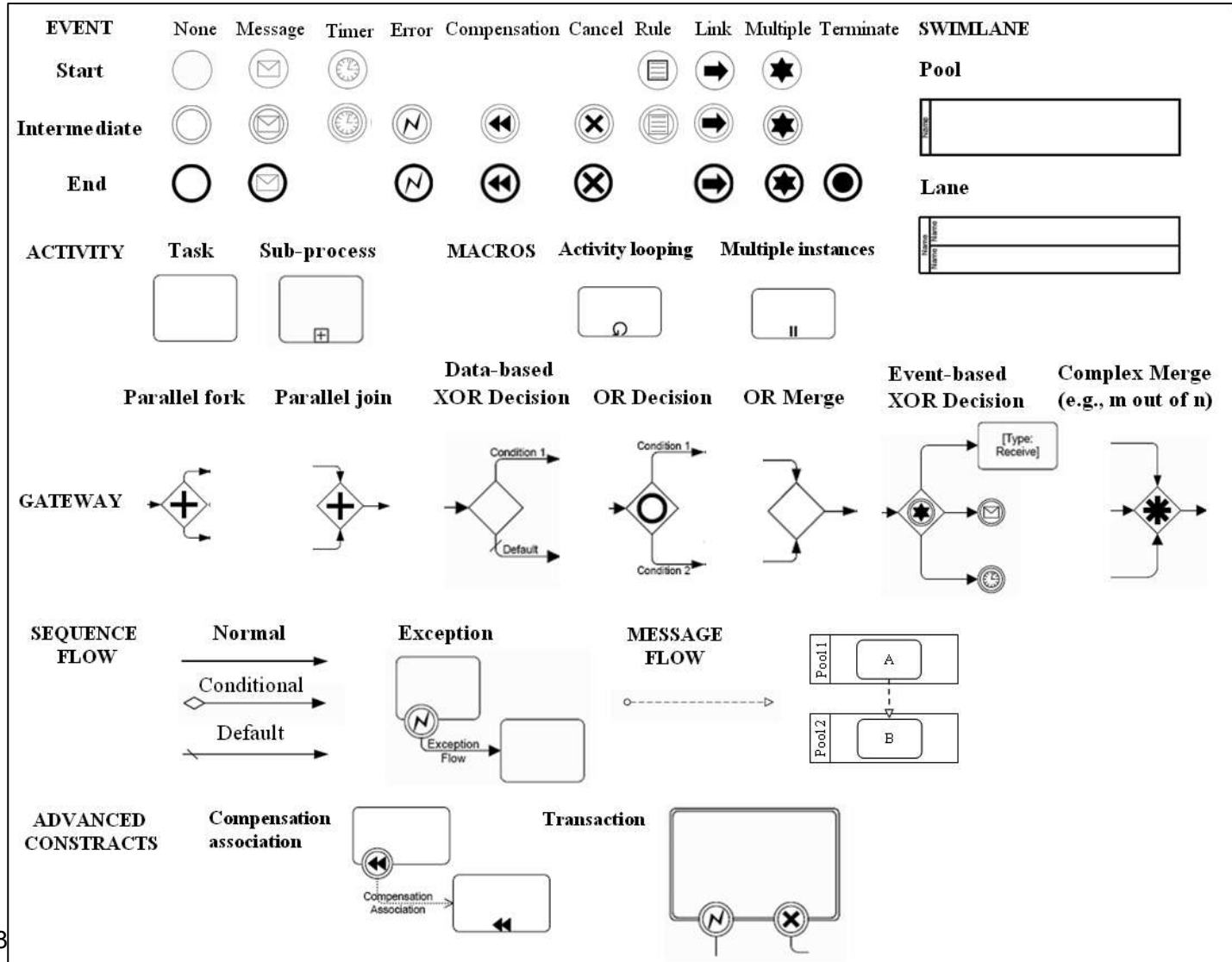


Introduction



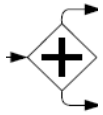
- Role of Formal Methods in SOA
- COMPAS Project
- Reo Coordination Language
- From Business Process Modeling (BPM) to Web Service (WS) Composition
 - BPMN to Reo mapping
 - Examples, process analysis
- Business Process Compliance Verification
 - Control flow, transactions, temporal requirements, Quality of Service (QoS)
- Conclusions and Future Work

BPMN

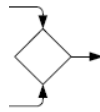
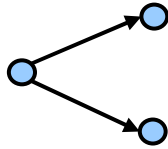




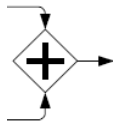
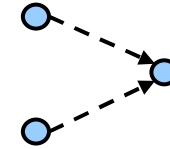
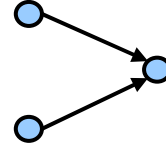
BPMN2Reo: basic gateways



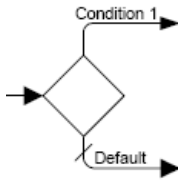
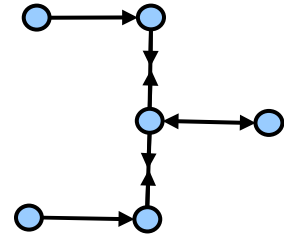
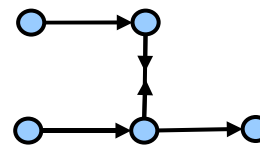
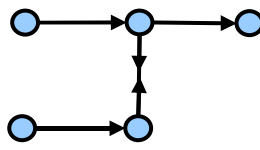
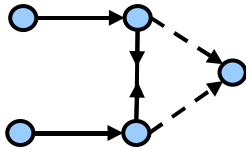
Parallel fork



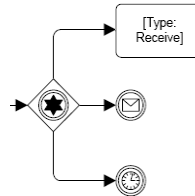
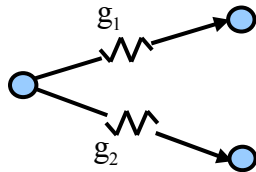
OR/XOR merge



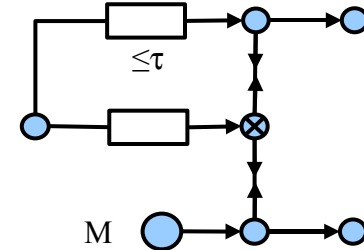
Parallel join



Data-based OR/XOR decision



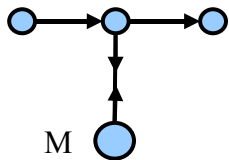
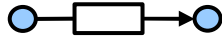
Event-based XOR decision



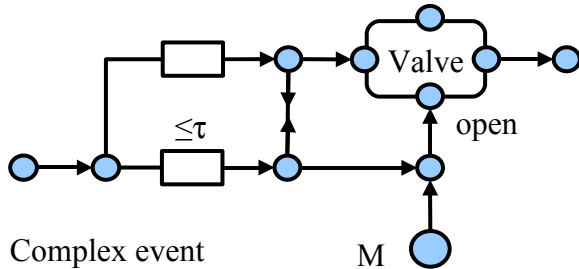
Complex gateways (e.g., m out of n choice) Repository of workflow patterns modeled with Reo <http://homepages.cwi.nl/~proenca/webreo/home.htm>



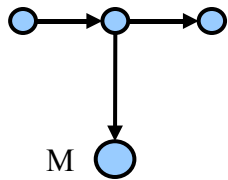
Atomic task



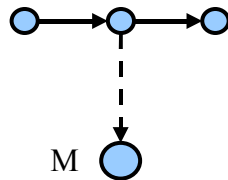
Message event



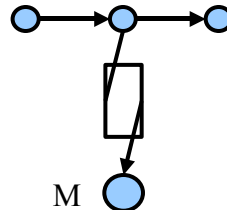
Complex event
(proceed if a message is received in a given time interval)



Blocking

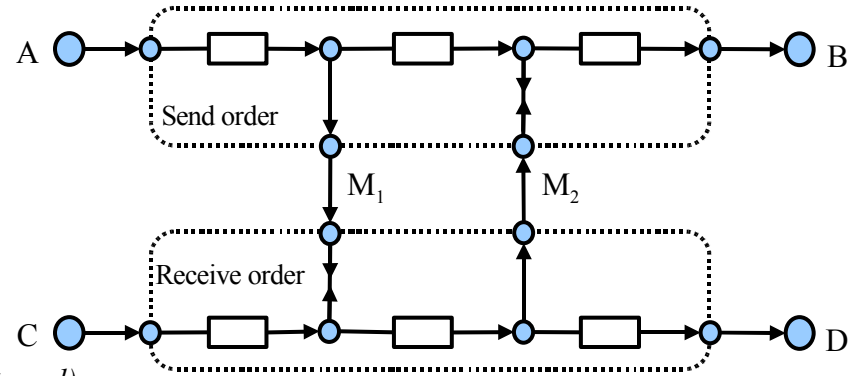


Non-blocking lossy

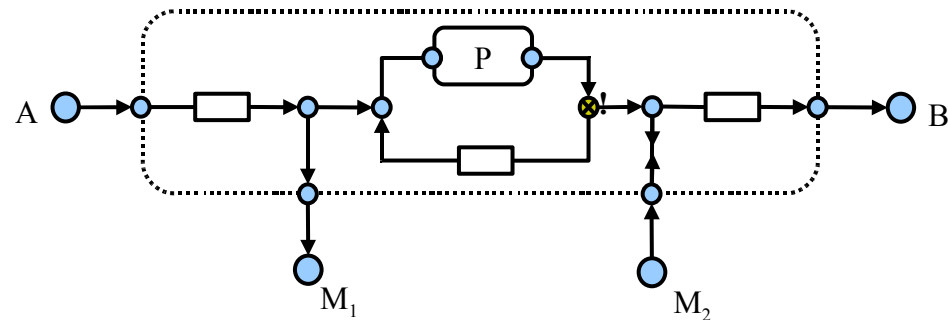


Non-blocking waiting

Outgoing messages

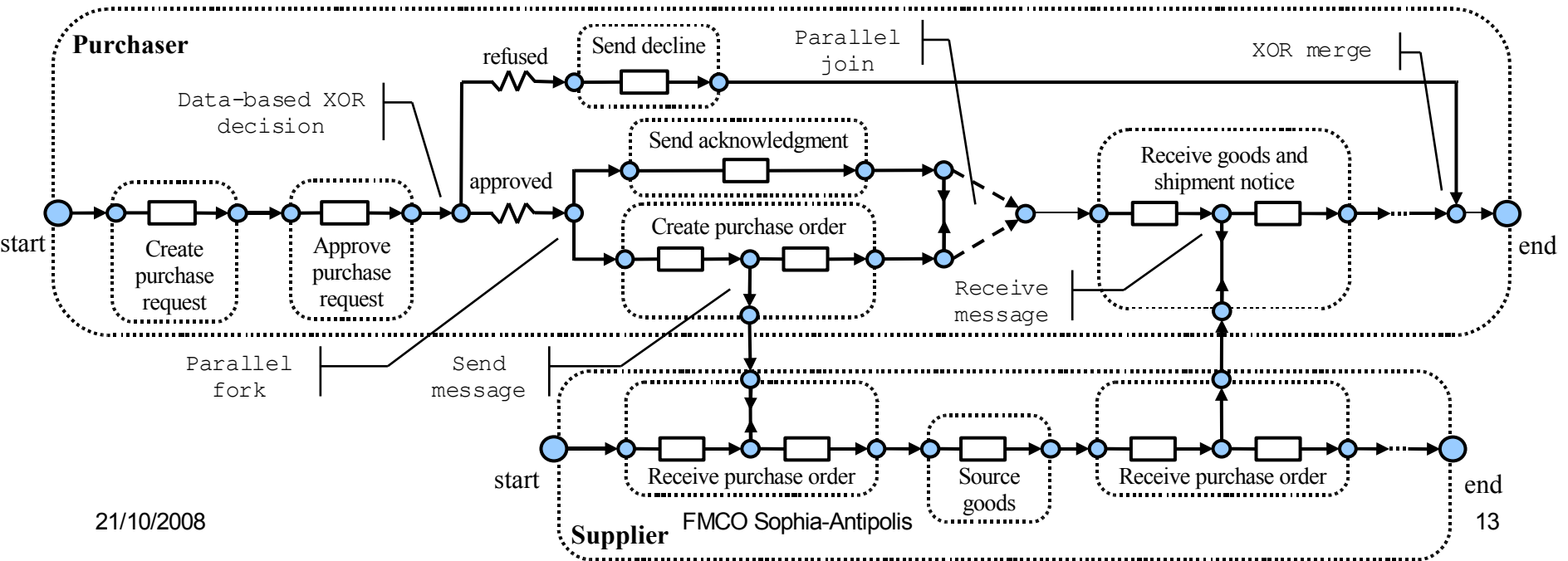
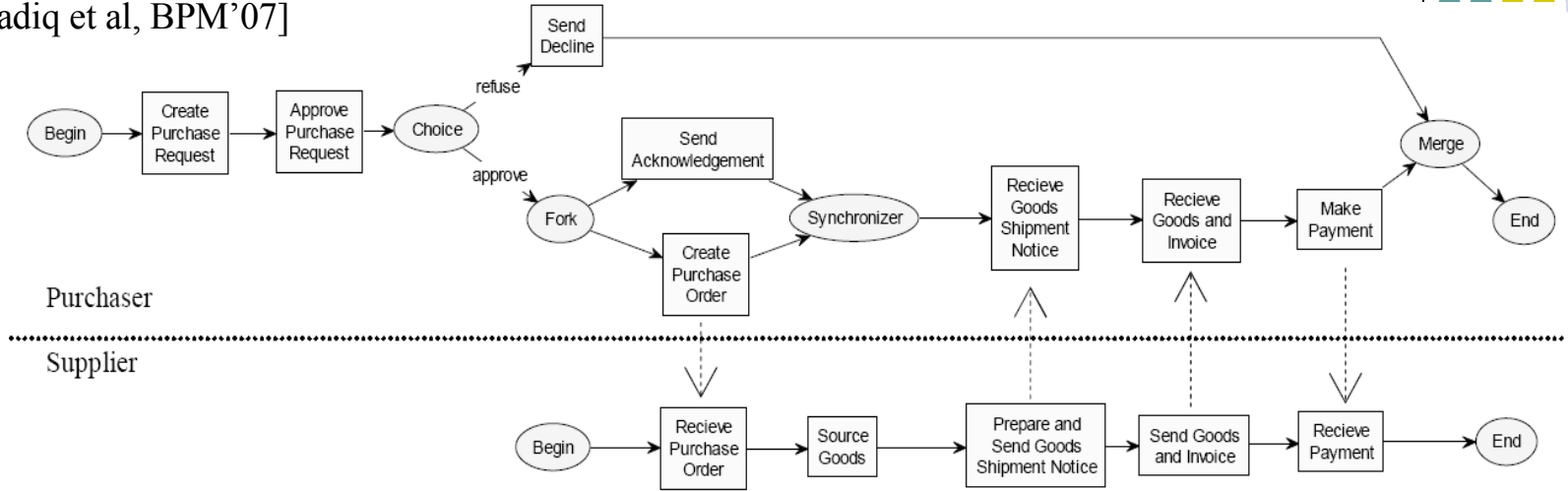


Synchronous message exchange



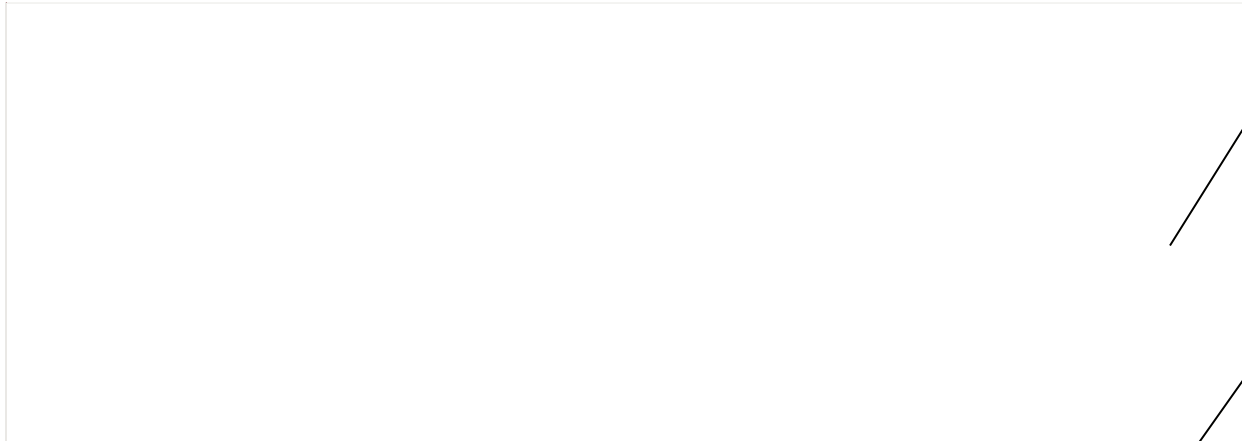


[Sadiq et al, BPM'07]





Business Process Design



1. BPMN diagram

2. Reo process model

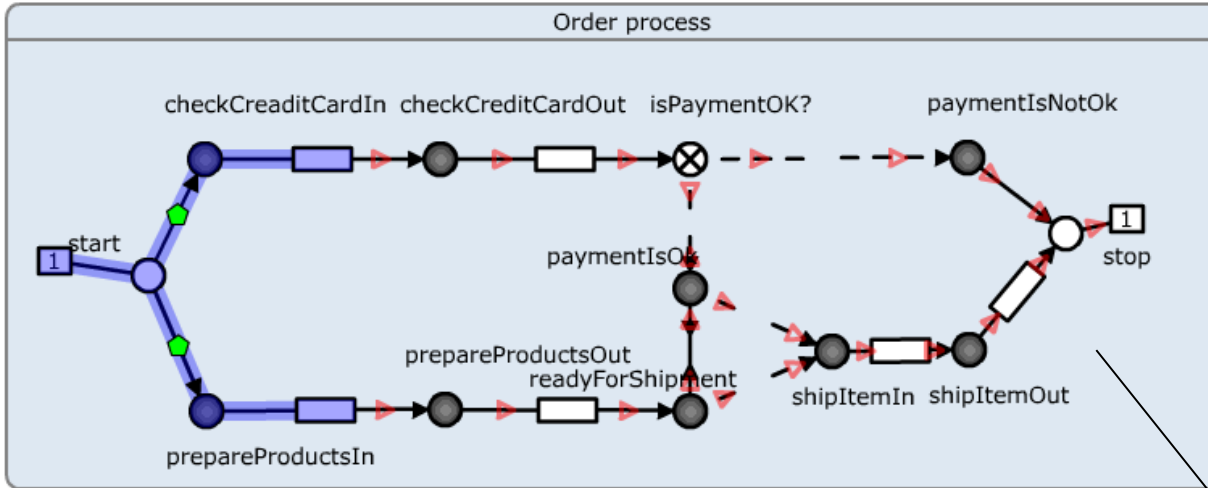
Business Process Analysis

List of animations

Animation 1
(5 steps)

Animation 2
(3 steps)

Animation 3
(3 steps)



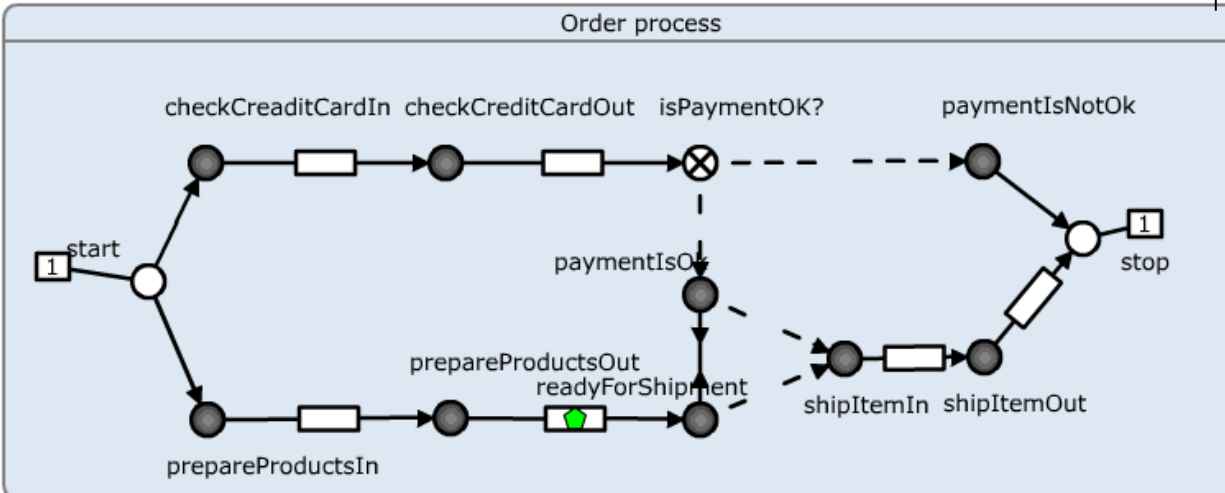
3. Reo animation

List of animations

Animation 1
(5 steps)

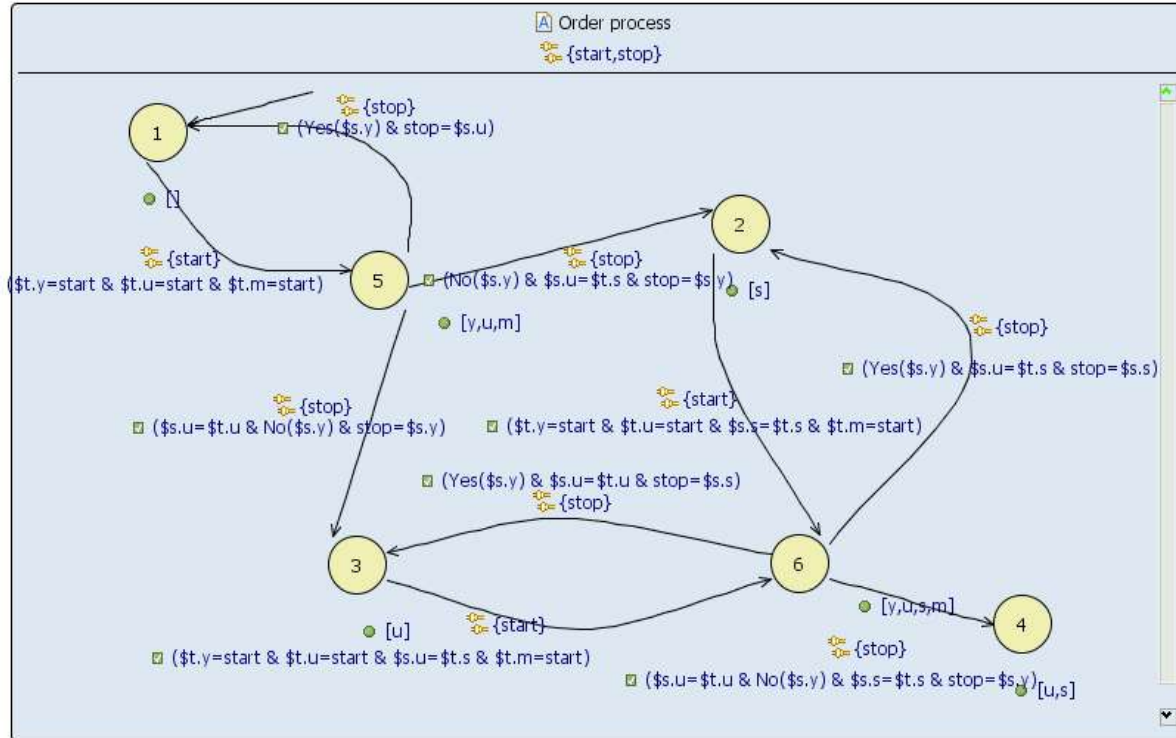
Animation 2
(3 steps)

Animation 3
(3 steps)





Business Process Analysis



QoS analysis with Quantitative Intentional Automata (QIA) –

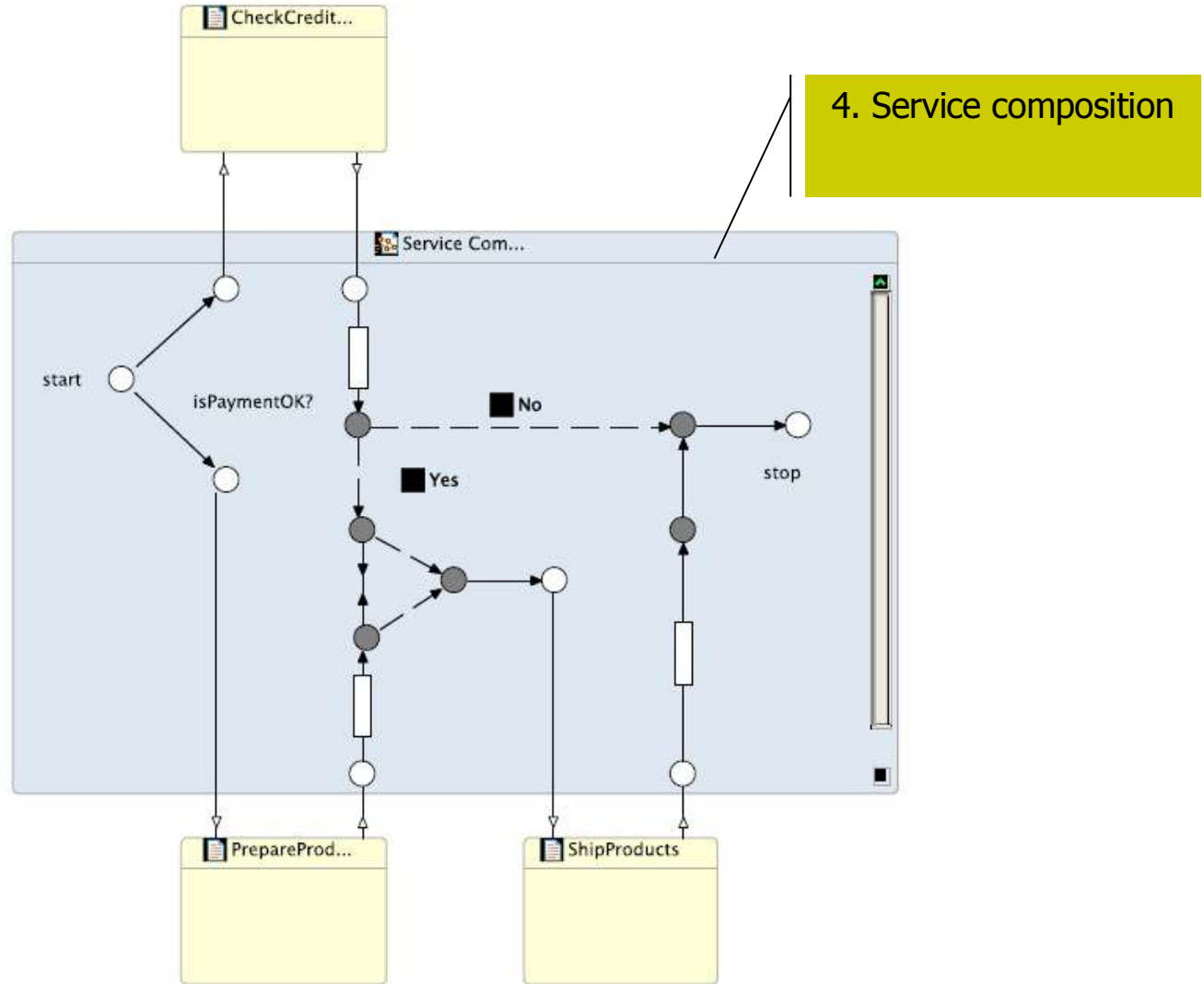
Constraint Automata with quantitative properties,

(e.g., arrival rates at ports and average delays of dataflows between ports).

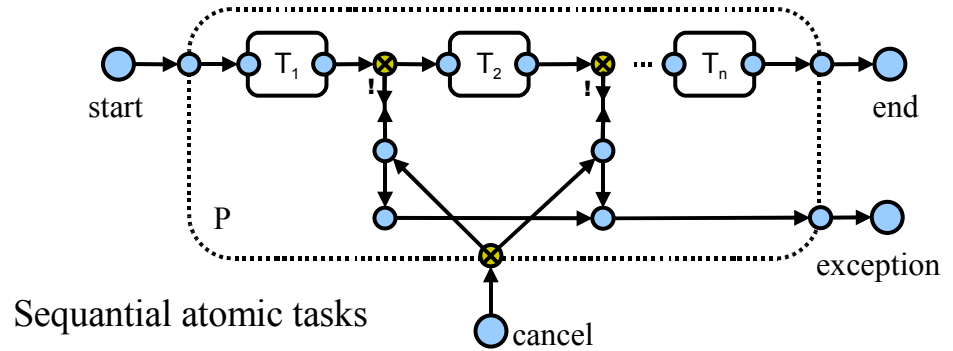
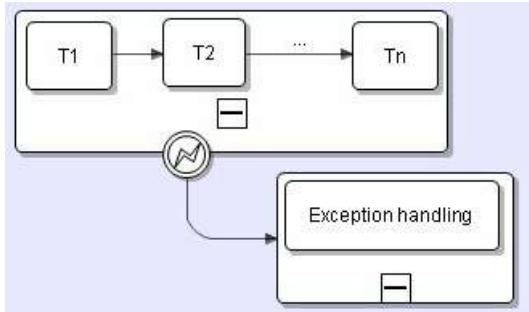
For performance analysis, these automata are translated to Continuous-Timed Markov Chains and fed into the PRISM model checker.



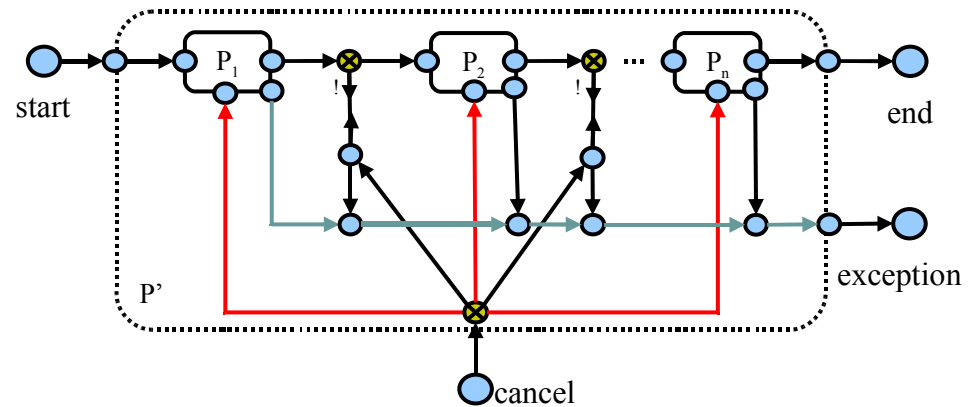
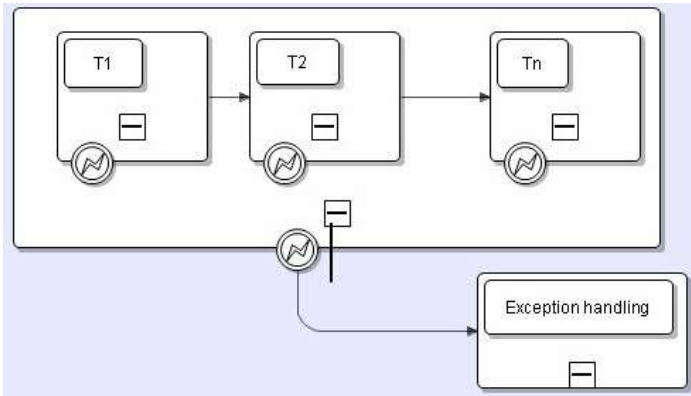
Web Service Composition



BPMN2Reo: Process termination and exception handling

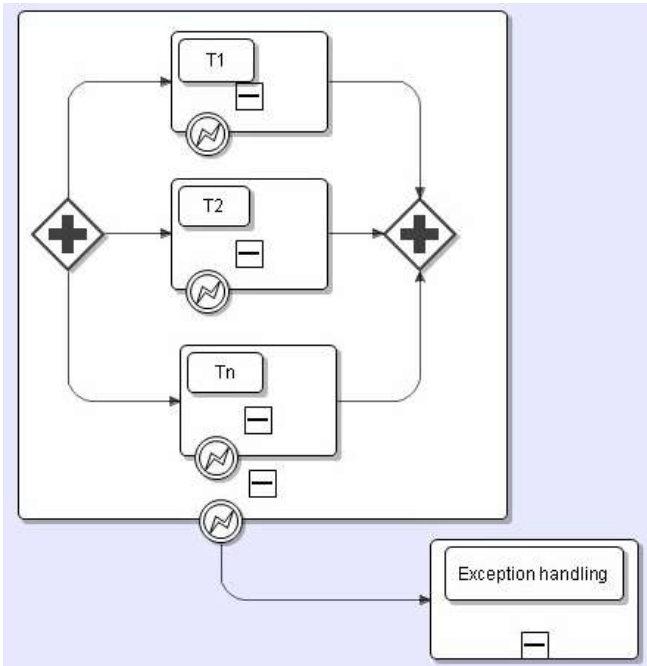


Sequential atomic tasks

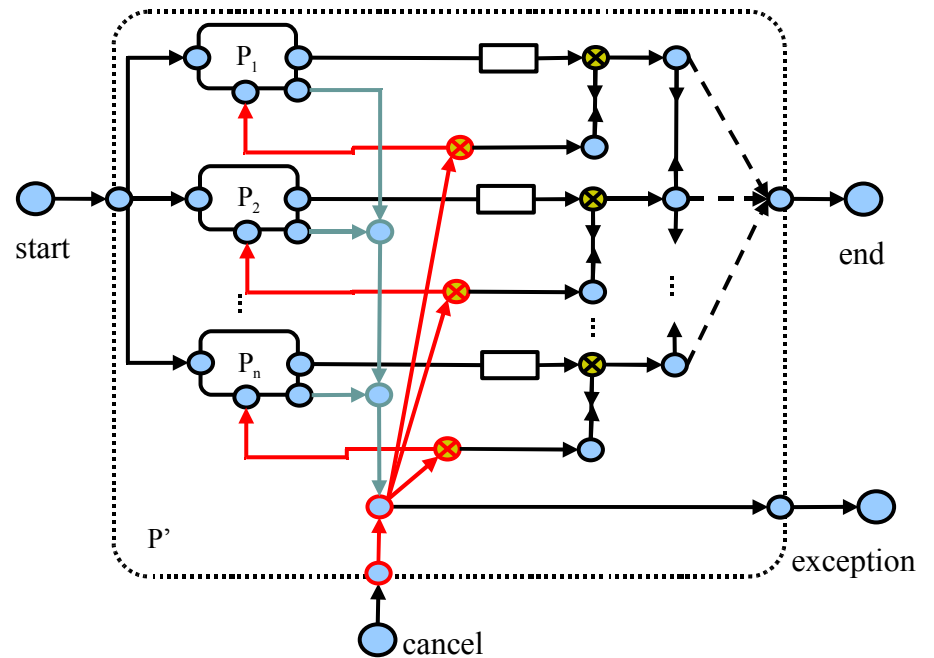


Sequential sub-processes

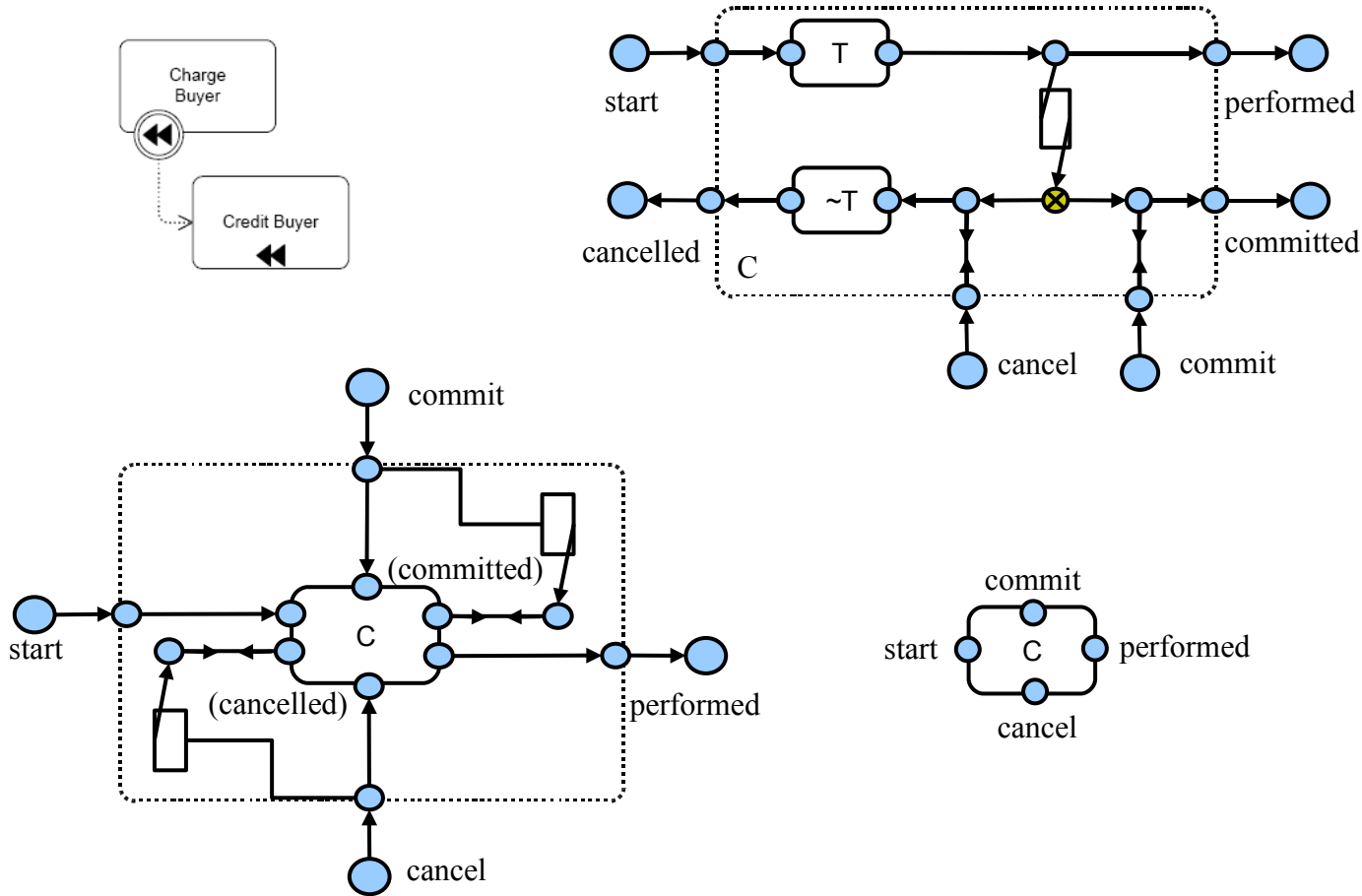
BPMN2Reo: Process termination and exception handling



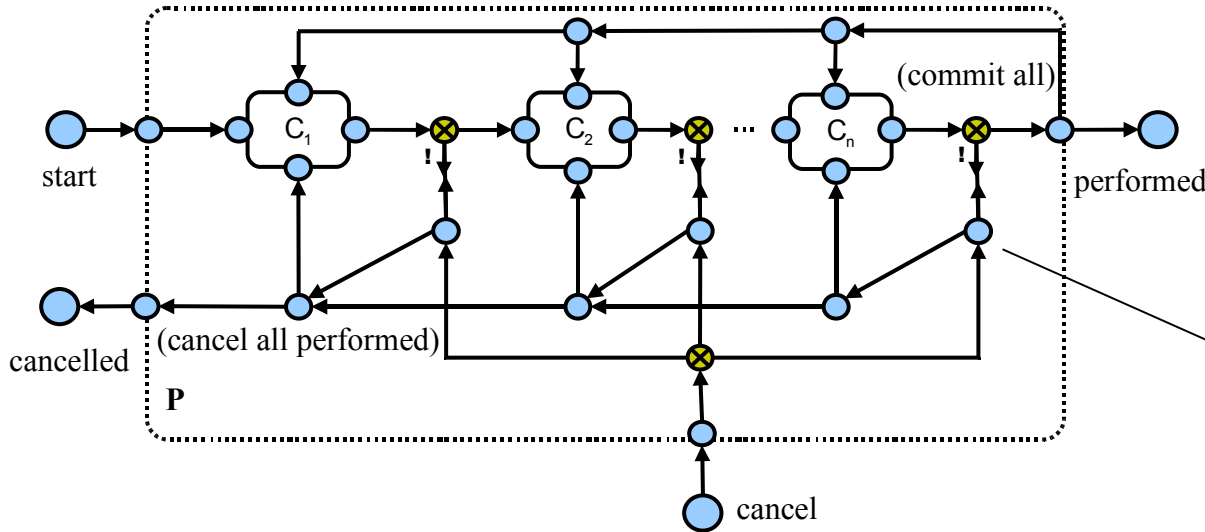
Parallel sub-processes



BPMN2Reo: Task compensation



Modeling Long Running Business Transactions in Reo

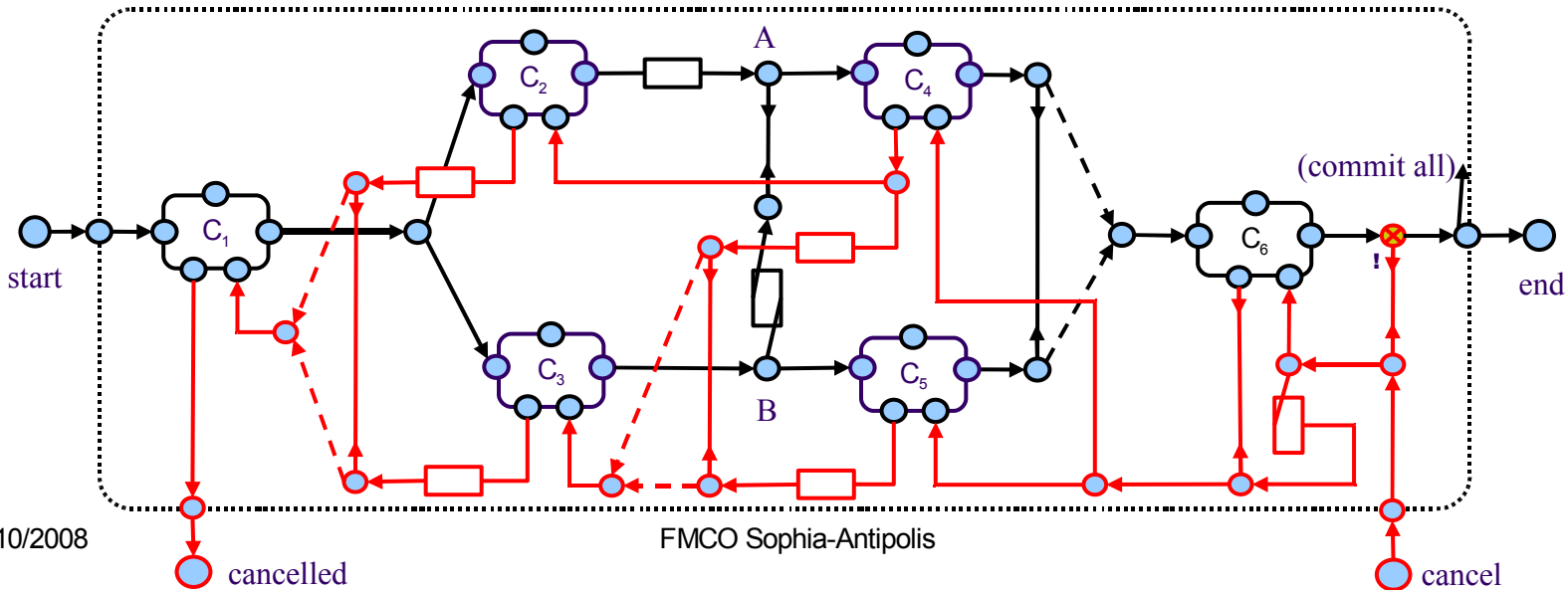
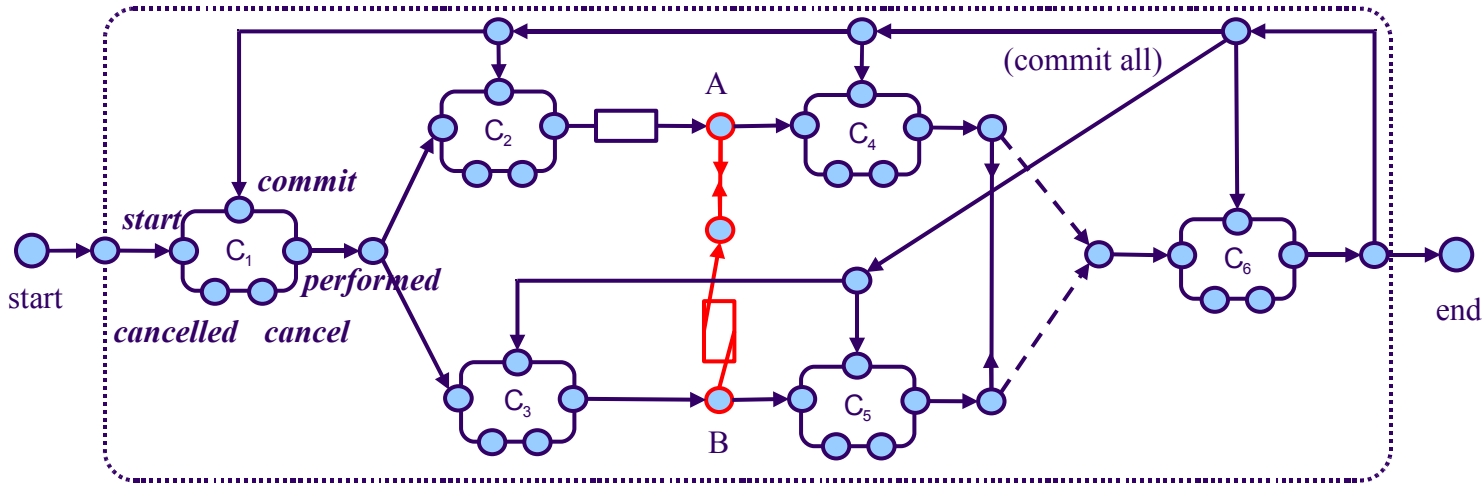


If a cancel message is received, the execution has to be stopped and all executed activities have to be compensated for

Encode in a CTL-like logic and automatically check common transaction properties like

- *Durability* (no more than one output is reached for any process run)
- *Eventuality* (an output is reached for any process run)
- *Atomicity* (all involved activities are either successfully completed or successfully canceled), etc.

Modeling Long Running Business Transactions in Reo





Business Process Compliance



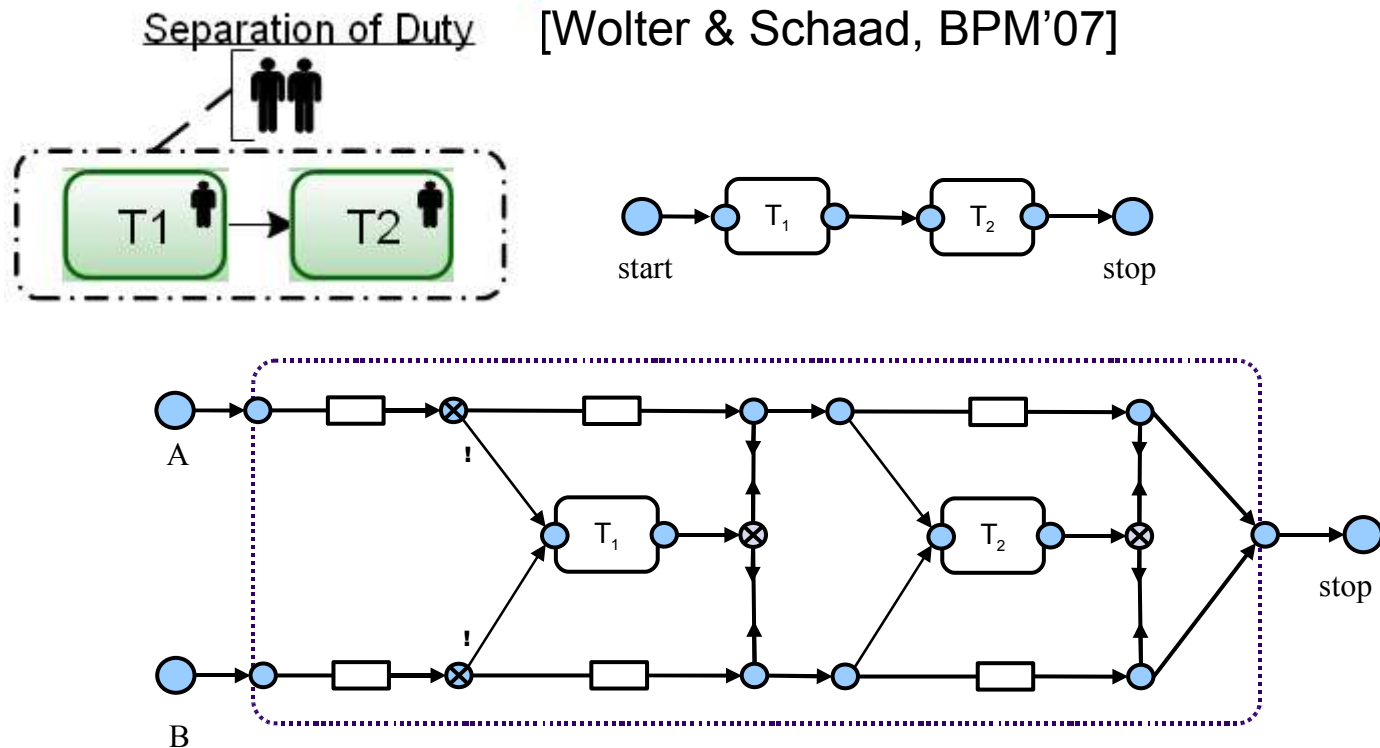
- COMPAS has identified
 - Control flow, locative, information, resource and temporal compliance concerns
 - Monitoring, payment, privacy, quality, retention, security and transaction compliance concerns
- We can deal (at least) with control flow, resource, temporal, quality and transaction compliance

Compliance-aware Business Process Design



- Separation of Duty (e.g., four-eyes principle)
 - One user cannot execute a whole process
 - E.g., 2 users must be involved in a process consisting of 4 sequential tasks
- Approach
 - Constraints on task assignment to users expressed in GMT extensions (e.g., BPMN) or DSLs
 - C. Wolter and A. Schaad “Modeling of Task-Based Authorization Constraints in BPMN”, BPM’07, volume 4714 of LNCS, Springer, pp. 64–79

Enforcing Separation of Duty Constraints

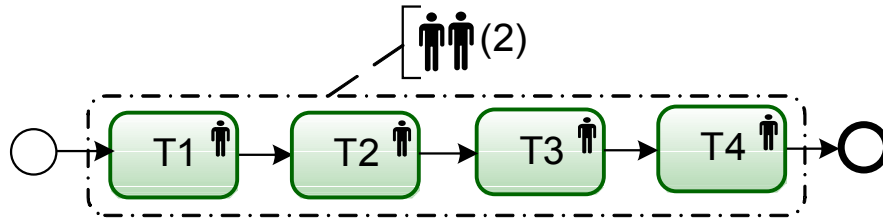


- Animation engine or model checking tools can be used to verify that tasks T₁ and T₂ are executed by different users
- Reo reconfiguration plug-in can be useful for process modification

Enforcing Separation of Duty Constraints

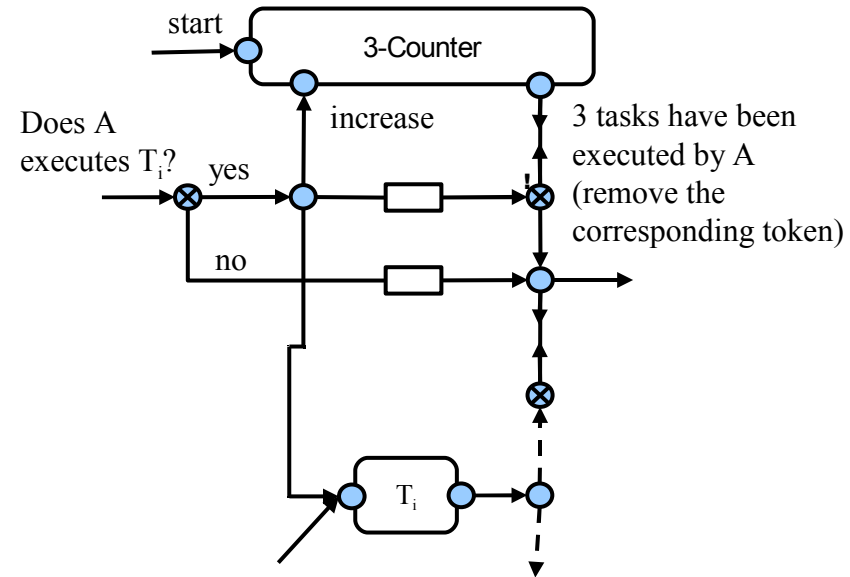
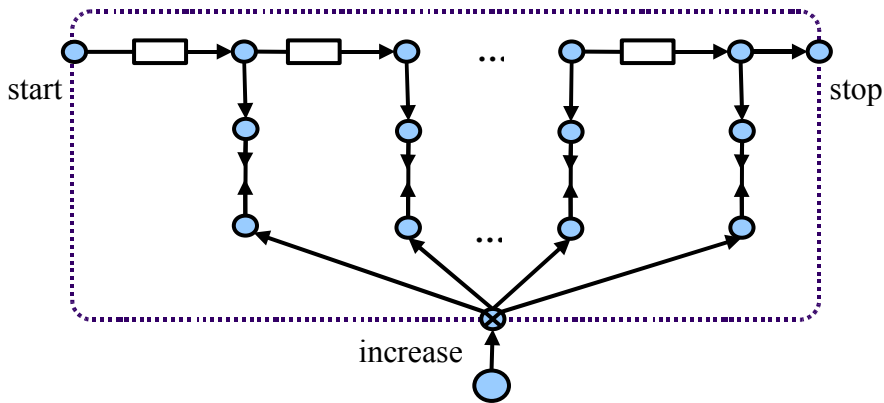


Operational Separation of Duty



[Wolter & Schaad, BPM'07]

3-Counter



(The same circuit for B)

Related Work



- BPMN semantics
 - Dijkman, R.M., Dumas, M., Ouyang, C.: Formal semantics and analysis of BPMN process models. In: Information and Software Technology (IST). (2008)
 - Wong, P., Gibbons, J.: A process semantics for BPMN. Technical report, Queensland University of Technology (2007)
 - Wong, P., Gibbons, J.: A relative timed semantics for BPMN. Technical report, Queensland University of Technology (2007)
- BPEL semantics
 - Lohmann, N.: A feature-complete Petri net semantics for WS-BPEL 2.0. In: Proc. of the Int. Workshop on Web Services and Formal Methods. Volume 4937 of LNCS., Springer (2008) 77-91
 - 11. Lucchia, R., Mazzara, M.: A pi-calculus based semantics for WS-BPEL. Journal of Logic and Algebraic Programming 70(1) (2007) 96-118
- Petri-net semantics for web service composition
 - Lohmann, N.: A feature-complete Petri net semantics for WS-BPEL 2.0. In: Proc. of the Int. Workshop on Web Services and Formal Methods. Volume 4937 of LNCS., Springer (2008) 77-91

Related Work



- Formal Methods for Compliance-aware Business Process Design
 - Liu, Y., Muller, S., Xu, K.: A static compliance-checking framework for business process models. IBM Systems Journal 46(2) (2007) 335-361
 - Ghose, A.K., Koliadis, G.: Auditing business process compliance. In: Proc. of the Int. Conf. on Service-Oriented Architectures (ICSOC'07). Volume 4749 of LNCS., Springer (2007) 169-180
 - Governatori, G., Milosevic, Z., Sadiq, S.: Compliance checking between business processes and business contracts. In: Proc. of the Int. Enterprise Distributed Object Computing Conf. (EDOC'06), IEEE Computer Society (2006) 221-232
 - Brunel, J., Cuppens, F., Cuppens, N., Sans, T., Bodeveix, J.P.: Security policy compliance with violation management. In: Proc. of the Workshop on Formal Methods in Security Engineering (FMSE'07), ACM Press (2007) 31-40
 - A. Awad, G. Decker and M. Weske, "Efficient Compliance Checking Using BPMN-Q and Temporal Logic", Proc. of the Int. Conf. on Business Process Management (BPM), 2008
- COMPAS Deliverable 2.1 "State-of-the-art in the field of compliance languages"

Reo/Constraint automata and their applications in SOC



- Arbab, F.: Reo: A channel-based coordination model for component composition. *Mathematical Structures in Computer Science* 14(3) (2004) 329-366
- Baier, C., Sirjani, M., Arbab, F., Rutten, J.: Modeling component connectors in Reo by constraint automata. *Science of Computer Programming* 61 (2006) 75-113
- Arbab, F., Baier, C., de Boer, F.S., Rutten, J.J.M.M.: Models and temporal logics for timed component connectors. *Int. Journal on Software and Systems Modeling* 6(1) (2007) 59-82
- Arbab, F., Koehler, C., Maraikar, Z., Moon, Y.J., Proenca, J.: Modeling, testing and executing Reo connectors with the Eclipse coordination tools. *Workshop on Formal Aspects in Component Software*, Elsevier (2008).
- Arbab, F., Chothia, T., Meng, S., Moon, Y.J.: Component connectors with QoS guarantees. In: *Proc. of the Int. Conf. on Coordination Languages (Coordination'07)*. Volume 4467 of LNCS., Springer (2007) 286-304
- Meng, S., F.Arbab: On resource-sensitive timed component connectors. In: *Proc. of the Int. Conf. on Formal Methods for Open Object-Based Distributed Systems (FMOODS'07)*. Volume 4468 of LNCS., Springer (2007) 301-316
- Meng, S., Arbab, F.: Web service choreography and orchestration in Reo and constraint automata. In: *Proc. of the ACM Symposium on Applied Computing (SAC'07)*, ACM Press (2007) 346-353
- S. Tasharofi, M. Vakilian, R. Z. Moghaddam and M. Sirjani, "Modeling Web Service Interactions Using the Coordination Language Reo", *Proc. of the Int. Workshop on Web Services and Formal Methods*, 2008, volume 4937 of LNCS, Springer, pp. 108-123

Conclusions and Future Work



- **Conclusions**
 - A formal behavioral model for business process / service composition description
 - Model-driven development – from high-level models to unambiguous executable models and their implementation
 - Processes are represented as Reo circuits or constraint automata
 - Compliance concerns are expressed as Reo circuits, constraint automata or logic formulae
- **Future Work**
 - Further investigation of compliance issues
 - Composition of processes from reusable compliant process fragments