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 II, Sarbanes-Oxley, IFRS2, MiFID, LSF4, HIPAA, Tabaksblat, 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

Business Process Lifecycle

Graphical Modeling Tools (GMT) (BPMN, UML2 ADs, BPEL)

BPMN2Reo,...

Reo/Constraint Automata
Modeling Tools

Code generation

Java, BPEL, WS-CDL, WSDL

Compliance Concerns

DSLs, GMT extensions

Constraints,
Temporal Logic Formulae,
Automata

Web Services, WS-Policies,
XACML, etc.
Reo Coordination Language

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

Exclusive choice (deferred XOR)
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. Tasharofii 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
BPMN2Reo: tasks, events and messages

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

Send order

Receive order

M₁

M₂

P

M₁

M₂
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
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

4. Service composition
BPMN2Reo: Process termination and exception handling

Sequential atomic tasks

Sequential sub-processes
BPMN2Reo: Process termination and exception handling

Parallel sub-processes

- Start
- P_1
- P_2
- P_n
- P'
- Exception handling
- Cancel
- End

21/10/2008

FMCO Sophia-Antipolis
BPMN2Reo: Task compensation
Modeling Long Running Business Transactions in Reo

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

[Wolter & Schaad, BPM’07]

Animation engine or model checking tools can be used to verify that tasks $T_1$ and $T_2$ are executed by different users.

Reo reconfiguration plug-in can be useful for process modification.
Enforcing Separation of Duty Constraints

Operational Separation of Duty


3-Counter

Does A executes $T_i$?

3 tasks have been executed by A (remove the corresponding token)

(The same circuit for B)
Related Work

- **BPMN semantics**

- **BPEL semantics**

- **Petri-net semantics for web service composition**
Related Work

- Formal Methods for Compliance-aware Business Process Design

- COMPAS Deliverable 2.1 “State-of-the-art in the field of compliance languages”
Reo/Constraint automata and their applications in SOC


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