Relations between case studies and Theme 2 results

– Towards D8.6 –

Maurice ter Beek

ISTI-CNR
Pisa, Italy

SENSORIA workshop
Pisa, 9–11 June 2008

Outline

Aim of SENSORIA Deliverable 8.6 (due M36)

Relations between case studies and Theme 2 results

D8.6 will describe the relations between the four SENSORIA case studies of WP8 and the more technical work as carried out within the WPs of Theme 2: *Mathematical analysis and verification techniques and tools for system behaviour and quality of service properties*

D8.6 will show how the theoretical approaches to qualitative and quantitative aspects of services (WP3 and WP4) are applied to scenarios of the Automotive, Finance, Telecommunications and Course management & e-learning case studies (WP8)

Towards D8.6: Eleven contributions collected on web site

⇒ Ten of them deal exclusively with the Automotive case study!!!

? One formalises a Finance scenario, but no analysis or verification technique or tool from WP3 or WP4 is used (does this fit D8.6?)

Aim of SENSORIA Deliverable 8.6 (due M36)

Relations between case studies and Theme 2 results

D8.6 will describe the relations between the four SENSORIA case studies of WP8 and the more technical work as carried out within the WPs of Theme 2: *Mathematical analysis and verification techniques and tools for system behaviour and quality of service properties*

D8.6 will show how the theoretical approaches to qualitative and quantitative aspects of services (WP3 and WP4) are applied to scenarios of the Automotive, Finance, Telecommunications and Course management & e-learning case studies (WP8)

Towards D8.6: Eleven contributions collected on web site

⇒ Ten of them deal exclusively with the Automotive case study!!!

? One formalises a Finance scenario, but no analysis or verification technique or tool from WP3 or WP4 is used (does this fit D8.6?)

Overview of collected contributions

- 11 contributions in total (10 $\times$ Automotive, 1 $\times$ Finance)
- 8 contributions from WP3 (Qualitative Aspects of Services),
  3 contributions from WP4 (Quantitative Aspects of Services)
- 1 contribution from T3.1, 2 from T3.2, 3 from T3.3, 2 from T3.4,
  1 from T4.2, 2 from T4.3
- ? T3.5: Language Extensions and Prototyping
- ? T4.1: Probabilistic and Stochastic Extensions of the Core Calculus
- ? T4.4: Resource Usage and Quantitative Security Issues
- Contributions from DSIUF, DTU, FAST, ISTI, LMU, LSS-IMPERIAL, PISA, S&N, UEDIN, ULEICES
- ? ATX, BUTE, FFCUL, LSS-UCL, MIP, UNIBO, UNITN, UWARSAW

  (some already announced their contributions during coffee breaks)

Formalising the S&N Credit Request (DTU & S&N)

- T3.1: Security and Trust for Services

- Finance: Credit request scenario
- Formalises scenario's cryptographic communication protocols
- Uses: Alice-Bob notation

- Results: Translate the case study from high-level formalism into low-level specifications in order to allow formal validation

- Future: Analyse security properties (confidentiality, authentication) to obtain full protocol analytical validation of system

Specifying and Analysing SOC Applications with COWS (DSIUF)

- T3.2: Resource Usage of Mobile Services

- Automotive: On road assistance scenario (a.k.a. low oil level)
- Flavour of qualitative properties that can be analysed with the tool
- Uses: COWS process calculus with additions (type system), SocL branching-time temporal logic, CMC on-the-fly model checker

- Results: Express and enforce confidentiality properties

- Future: Enable the use of proof techniques and analytical tools developed for COWS to analyse SOC applications programmed in WS-BPEL or modelled in SRML

Relational Analysis for Delivery of Services (DTU)

- T3.2: Resource Usage of Mobile Services

- Automotive: Accident assistance scenario (a.k.a. airbag)
- Static analysis in relational form
- Uses: pπ pattern-matching π-calculus, flow logic

- Results: Ensure the correct delivery of services in the presence of multiplexed communication; used to show that only service subscribers are able to employ a service

- Future: Transfer the analysis technology to the richer set of Sensoria core calculi

Relational Analysis of Correlation (DTU)

- T3.3: Behavioural Properties

- Automotive: Accident assistance scenario (a.k.a. airbag)
- Static analysis in relational form of correlations
- Uses: CWS fragment of COWS process calculus (orchestration constructs discarded), flow logic

- Results: Proof of absence of malign session interference

- Future: Add orchestration constructs (discarded from COWS)

A flow-sensitive analysis of privacy properties (DTU)

- T3.3: Behavioural Properties

- Automotive: On road assistance scenario (essentially)
- Flow-sensitive and context-sensitive analysis of π-calculus
- Uses: Static program analyses techniques, π-calculus

- Results: Ensure that private information sent to services over a wireless network is not leaked

- Future: Develop similar analysis technique for hardware programming language VHDL

Logic-based conflict detection for distributed policies (PISA & ULEICES)

- T3.3: Behavioural Properties

- Automotive: On road assistance scenario (a.k.a. car repair)
- Semantics-based techniques to detect policy conflict and a consideration of conflict resolution
- Uses: Appel policy language, theorem proving, ΔDSTL(x) distributed-state temporal logic

- Results: Detection of conflicts

- Future: Implement conflict detection filter using the proof assistant MaRK (built on top of Isabelle)

Formal Verification of an Automotive Scenario in SOC (ISTI & LMU/FAST)

- T3.4: Verification Techniques

- Automotive: On road assistance scenario (a.k.a. low oil level)
- Qualitative analysis of the scenario's requirements model
- Uses: UML, communicating UML state machines, CMC on-the-fly model checker, SocL action- and state-based branching-time temporal logic

- Results: The requirements model of the scenario is well designed

- Future: relax modelling assumptions, perform quantitative analysis

A model checking approach for verifying COWS specifications (DSIUF & ISTI)

- T3.4: Verification Techniques

- Automotive: On road assistance scenario (a.k.a. low oil level)
- Qualitative analysis of properties of services expressed as generic logical patterns describing desirable peculiar features of services
- Uses: COWS process calculus, SocL branching-time temporal logic, CMC on-the-fly model checker

- Results: Express and check functional properties of services

- Future: Define an alternative operational semantics for COWS to support a more compositional verification methodology

Stochastic Logics (DSIUF & ISTI)

- T4.2: Stochastic Logics

- Automotive: Accident assistance scenario (a.k.a. airbag)
- Towards quantitative analysis (no model checking yet)
- Uses: MoSL action- and state-based real-time probabilistic spatial temporal logic (for StoKlaim)

- Results: Express non-functional, performance and dependability oriented properties/requirements of/on services

- Future: Develop proper tools to support system modelling and verification based on StoKlaim and MoSL

Evaluating Quality of Service for Service Level Agreements (UEDIN)

- T4.3: Quantitative Measurements of QoS for SLAs

- Automotive: Accident assistance scenario (a.k.a. airbag)
- Quantitative analysis of QoS metrics
- Uses: Cyclic PEPA process algebra, Stochastic Petri Nets (via ipc Imperial PEPA compiler), Hydra DNAmaca Markov chain analyser (SPN tool), Condor high-throughput computing platform

- Results: Sensitivity (response-time) analysis of above scenario

- Future: Better use Condor's support for distributed computing

Safety and Response-Time Analysis of an Automotive Accident Assistance Service (LSS-IMPERIAL, UEDIN & LMU)

- T4.3: Quantitative Measurements of QoS for SLAs

- Automotive: Accident assistance scenario (a.k.a. airbag)
- Qualitative and quantitative analysis
- Uses: FSP Finite State Process notation, PEPA process algebra, LTSA Labelled Transition System Analyzer, SDE Sensoria Development Environment (e.g. PEPA Eclipse Plug-in project and ipclib tool suite)

- Results: Safety and response-time analysis of above scenario

- Future: Extend the SDE to perform analyses on high-level (UML or BPEL) models

Work to be done...

Applications of Theme 2 results to the other case studies? (Finance?)

i.e. of analysis/verification techniques & tools from WP3/WP4 to WP8

Send me a 1–2 page contribution to D8.6!
(if you did not do so already...)

See Laura's talk for a template structure for your contribution

and

see Nora's talk for the deadline for sending your contribution

Work to be done...

Applications of Theme 2 results to the other case studies? (Finance?)

i.e. of analysis/verification techniques & tools from WP3/WP4 to WP8

Send me a 1–2 page contribution to D8.6!
(if you did not do so already...)

See Laura's talk for a template structure for your contribution

and

see Nora's talk for the deadline for sending your contribution

Work to be done...

Applications of Theme 2 results to the other case studies? (Finance?)

i.e. of analysis/verification techniques & tools from WP3/WP4 to WP8

Send me a 1–2 page contribution to D8.6!
(if you did not do so already...)

See Laura's talk for a template structure for your contribution

and

see Nora's talk for the deadline for sending your contribution