assessability

from resilience-building to resilience-scaling technologies: directions

ReSIST 2nd Open Workshop, Rome, Oct. 2007

contributors

Cinzia Bernardeschi,
Peter Bokor,
Andrea Bondavalli,
Marc Dacier,
Colin O'Halloran,
Mohamed Kaâniche,
Karama Kanoun,
Marc-Olivier Killijian,
Jean-Claude Laprie,
Giuseppe Lettieri,
Bev Littlewood,
Paolo Lollini,
István Majzik,
Nick Moffat,
Alberto Pasquini,
Péter Pásztor,
Holger Pfeifer,
Peter Popov,
James Riordan,
Nicolas Rivière,
Yves Roudier,
Matthieu Roy,
Lorenzo Strigini,
Neeraj Suri,
Aad van Moorsel,
Hélène Waeselynck

research topics

GA1 - Integration of modelling in the engineering process
GA2 - Data selection, collection, validation
GA3 - Dependability cases
GA4 - Security quantification
GA5 - Benchmarking
GA6 - Model complexity
GA7 - Metrics/models for evolution processes
GA8 - Evaluation of dynamic systems
GA9 - On-line assessment for resilience
GA10 - Trust and cooperation
GA11 - Verification of mobile computing systems
GA12 - Abstraction
GA13 - Test methods for aspect-oriented systems
GA14 - Compositional reasoning
GA15 - Emergent behaviours in large-scale socio-technical systems
GA16 - Modelling effect of micro-decisions In the whole system
GA17 - Modelling human behaviour
GA18 - Inter-organisation boundary failures

Assessability

from the project proposal:

motivated by:

"... the fact that current and future systems result from evolutions of pre-existing systems, and, as a consequence, to move from off-line, pre-deployment assessment to continuous automated and operational assessment. "

roughly defined as:

"the ability to assess their ability to function properly and the quality of service that they will deliver"

with challenges (as anticipated in 2004) in:

- metrics
- mathematical modelling
- observability
- assessable architecture
- argument structuring and confidence

system perspective

characteristics:

- evolvable
- pervasive, mobile
- heterogeneity in scale: small devices, large servers
- everything inter-networked, dynamic coalitions
- new programming approaches

implication for assessability:

- evolving requirements
- large models
- stiff models
- on-line assessment
- self-similarity, chaos

system perspective

two main returning issues in assessability of evolving systems

1. how to assess the impact of **human** behaviour (user, operator)?
   - need for models of human behaviour
     - ✓ malicious behaviour
     - ✓ accidental failures
     - ✓ [illegible]
   - how to involve humans in test beds, e.g. in mobile systems ('living labs')
2. how to deal with ever increasing **complexity**
   - on-line solution of formal models, improve composition, abstraction
   - how to measure complex systems, identify emerging behaviour, characterise its complexity, etc.
   - conventional modelling approaches break down in chaotic, self-similar systems

methods & techniques perspective

how do our known methods and techniques (model checking, monte-carlo simulation, Petri net modelling, ...) hold up?

in addition to the complexity challenge, two main issues stand out

1. how to include **stakeholder** perspective (user, business, regulator)?
   - need for higher-level modelling paradigms for various perspectives
   - need for integration of new modelling approaches: game-theoretic, risk analysis, ...
   - how to deal with the sensitivities around benchmarking
2. how to measure and model **security**
   - development of a security metric
   - models of threats, impact, analysis of risk

engineering discipline perspective

why is assessment not an integral part of computer system design, deployment and operation?

we urge for new contributions in:

- resilience **benchmarking**
- **dependability case** construction and argumentation
- inclusion of assessability techniques in **model-driven design** and domain languages
- **demonstration vehicles**

challenge increases: evolving systems implies we must move from design to deployment and operation

assessability conclusion

extensive analysis of research challenges, greatly refining and completing the anticipated challenges

identified the following foci:

- system: *human behaviour* and *complexity*
- methods & techniques: *stakeholder perspective* and *security models & metrics*
- engineering discipline: overarching driver

contributors

Cinzia Bernardeschi,
Peter Bokor,
Andrea Bondavalli,
Marc Dacier,
Colin O'Halloran,
Mohamed Kaâniche,
Karama Kanoun,
Marc-Olivier Killijian,
Jean-Claude Laprie,
Giuseppe Lettieri,
Bev Littlewood,
Paolo Lollini,
István Majzik,
Nick Moffat,
Alberto Pasquini,
Péter Pásztor,
Holger Pfeifer,
Peter Popov,
James Riordan,
Nicolas Rivière,
Yves Roudier,
Matthieu Roy,
Lorenzo Strigini,
Neeraj Suri,
Aad van Moorsel,
Hélène Waeselynck