An Architectural Support for Self-Adaptive Software for Treating Faults

Rogério de Lemos
University of Kent, UK

José Luiz Fiadeiro
University of Leicester, UK

- Context
- Fault tolerance
- Computation, coordination and configuration
- Dynamic reconfiguration
- Concluding remarks
**Context**

- What does "self healing" mean to you?
  - Fault tolerance – a means to achieve dependability;
- What part of the self-healing problem are you dealing with?
  - Fault treatment at the architectural level;
- What part are you not dealing with?
  - Error processing;
- What applications are you targeting?
- What are the top two/three new technical ideas/approaches:
  - Structural adaptability - separation between computation and coordination for the provision of flexible structures;
  - Behavioural adaptability - immune inspired fault tolerance;
Fault Tolerance

The undesired - but in principle expected - circumstances that affect the dependability of systems:

\[
\bullet \bullet \bullet \rightarrow \text{failure} \rightarrow \text{fault} \rightarrow \text{error} \rightarrow \text{failure} \rightarrow \text{fault} \rightarrow \bullet \bullet \bullet
\]

*Fault tolerance* - the provision of services in spite presence of faults;

- *Error processing* - detection, damage assessment, and recovery;
- *Fault treatment* - diagnosis, and repair;

Fault assumptions in terms of *nature* and *rate*;
Idealised Fault Tolerant C2 COTS (iCOTS)
Fault Treatment

Isolation of the faults is obtained by *dynamic reconfiguration*:

- availability of redundancies;
- ability to modify system structure;
- definition of acceptable but less desirable levels of service;
  - diversity of services for certain class of failures;
Proposed Architecture

Computation: manages computations performed by components;

Coordination: enforces the interactions between components;

Configuration: determines when and how the components and connectors should be linked;
Co-operative Architectural Style

connector name
  attributes
  roles
  behaviour
    initial
    pre-condition
    normal
      invariant
      operation
      post-condition
  exceptional
    signal
    handler
    post-condition
  failure
    omission
    commission
Fault Treatment

Dynamic reconfiguration is obtained by:

- selecting different components and collaborations;
- sequence of atomic transactions achieving stability;
Dynamic Reconfiguration
Concluding Remarks

Architectural support for dependability:
- definition/identification of structuring concepts, mechanisms and techniques that provide flexibility for supporting run-time adaptability;

Some challenges:
- identification of service redundancies;
- instantiation of reconfiguration policies into strategies;
- realization of the strategies without service disruption;
- techniques for evaluating configuration strategies;
Concluding Remarks

Immune inspired fault tolerance:

- looking for learning capabilities support that may be able to deal with *unexpected* circumstances:
- it removes the *predictability* aspect;
  - can these learning capabilities be trusted?
  - how to protect the system from undesirable decisions?