

WICSA 07 Tutorial

Architecting Fault Tolerant Systems
H. Muccini, P. Pelliccione, A. Romanovsky
January 7, 2007, (Half Day – PM)

Architecting Fault Tolerant Systems (Tutorial Overview)

H. Muccini, P. Pelliccione
Dipartimento di Informatica
University of L'Aquila, Italy
[muccini,pellicci]@di.univaq.it

A. Romanovsky
Center for Software Reliability
University of Newcastle upon Tyne - UK
alexander.romanovsky@ncl.ac.uk

Fault tolerance, being one of the four means for guaranteeing dependability, is intended to ensure the delivery of the correct services in the presence of active faults. It is implemented by *error detection* and subsequent *system recovery*. Error detection finds an erroneous system state. Following system recovery transforms the system state that contains one or more errors and (possibly) faults into a state without detected errors and faults (fault handling). Exceptions and exception handling provide a general framework for structuring the fault tolerance activities in a system, by focusing on the concept of exceptional/abnormal behaviour (as opposed to normal behaviour), exception handling enables specifying actions to be undertaken in the presence of abnormal events.

While typical solutions focus on fault tolerance (and specifically, exception handling) during the design and implementation phases of the software life-cycle (e.g., Java and Windows NT exception handling), more recently the need for explicit exception handling solutions during the entire life cycle has been advocated by some researchers. Several solutions have been proposed for fault tolerance via exception handling at the software architecture and component levels.

This tutorial describes how the two concepts of fault tolerance and software architectures have been integrated so far. It is structured in two parts (*Overview on Fault Tolerance and Exception Handling*, and *Integrating Fault Tolerance into Software Architecture*) and is based on a survey study on architecting fault tolerant systems where more than fifteen approaches have been analyzed and classified. The tutorial concludes identifying those issues that remain still open and require deeper investigation.