An Idealized Fault-Tolerant Architectural Component

Paulo Asterio de C. Guerra
Cecília Mary F. Rubira
Instituto de Computação
Universidade Estadual de Campinas, Brazil

Rogério de Lemos
Computing Laboratory
University of Kent at Canterbury, UK
Motivation

- Reliable Component-Based Systems

Unreliable Components

Fault Tolerant Architecture
Objectives

- To apply the concept of “idealized fault tolerant component” for describing fault-tolerant component-based systems, at the architectural level.

- C2 architectural style
  - Heterogeneous COTS
  - Broadcasting of asynchronous messages
The Idealized Fault-Tolerant Component

Normal Behaviour
- Request
- Normal Response
- Interface Exception
- Failure Exception

Abnormal Behaviour
- Internal Exception

Return to Normal
The C2 Architectural Style

- Component
- Connector
- Request
- Notification
Proposed Architecture

- An idealized C2 component (iC2C)
  - Structure and behaviour as defined by the idealized fault-tolerant component (iFTC).
  - Fully compliant with the C2 style rules.
Overall Structure

- **iC2C top**
  - Normal activity
- **iC2C internal**
  - Abnormal activity
- **iC2C bottom**
  - Error diagnosis & recovery

**Normal behaviour & Error detection**

**Error diagnosis & recovery**
Overall Structure

iC2C top

NormalActivity

iC2C internal

AbnormalActivity

iC2C bottom

State based message routing

Serializes requests
Normal Message Flow

iC2C top

NormalActivity

iC2C internal

AbnormalActivity

iC2C bottom

Service Request

Request
Normal Message Flow

- iC2C_top
  - NormalActivity
  - iC2C_internal
    - AbnormalActivity
  - iC2C_bottom

Normal Response
Normal Message Flow

- iC2C_top
  - NormalActivity
- iC2C_internal
  - AbnormalActivity
- iC2C_bottom
Abnormal Message Flow

- **iC2C top**
- **iC2C internal**
- **iC2C bottom**

- **NormalActivity**
- **AbnormalActivity**

- **External Exception**

- **Internal Exception**

- **Abnormal Message Flow**
Abnormal Message Flow

- iC2C_top
- NormalActivity
- iC2C_internal
- AbnormalActivity
- iC2C_bottom

- Normal Response
- Return to normal
- Failure Exception

- Exception
- Normal
- Abnormal Message Flow
The NormalActivity Component

The NormalActivity Component implements operations and coordinates error detection.

Pre- and post-conditions checking
The NormalActivity Component

- **normal_top**
  - BasicNormal
  - Collaborating Component

- **normal_bottom**
  - Stores request
  - Evaluates pre-condition
The NormalActivity Component

- BasicNormal
- Collaborating Component
- Interface Exception

Accepts the request
(or)
C2 Integration

C2 Comp

iC2C_top
NormalActivity

iC2C_internal
AbnormalActivity

iC2C_bottom

C2 Comp

iC2C_top
NormalActivity

iC2C_internal
AbnormalActivity

iC2C_bottom
C2 Integration

- iC2C_top
  - NormalActivity
- iC2C_internal
  - AbnormalActivity
- iC2C_bottom

AbnormalActivity
Example – Mine Pump Control System

- Fault Model
  - Transient faults affecting pump

- Error Detection
  - Test water flow sensor (reliable)

- Error Recovery
  - Retry operation
Subsystem Configuration

conn1

LowWater Sensor

conn2

Ideal Pump

PumpControl Station

conn3

Structured as an iC2C
Ideal Pump Structure

Test Water Flow Sensor after pump on / off operation.

Recover by retry.
Normal pumpOn

pumpOn request

pumpOn notification

Pump

WaterFlow Sensor

Pump_Normal_top

Pump_Normal_bottom

PumpAbnormal

iP_top

iP_internal

iP_bottom
Normal pumpOn

- iP_top
- iP_internal
- iP_bottom

Pump

- Pump_Normal_top
- Pump_Normal_bottom

WaterFlow Sensor

PumpAbnormal

send notification

test sensor status

send notification
Error Detection

- iP_top
- Pump_Normal_top
- WaterFlow_Sensor
- Pump_Normal_bottom
- iP_internal
- PumpAbnormal
- iP_bottom

- test sensor status
- raises internal exception

- Pump комис太平洋
- WaterFlow Sensor
- Pump_Normal_top
- iP_top
Error Recovery

- successfull pumpOn notification
- return to normal
- send notification
- retry pumpOn
Main Results

- Idealized fault-tolerant component concept applied at the architectural level of C2 style systems

- Results may be adapted for other styles of the “interacting processes style category”
Work in Progress

- Idealized C2 connector
- FTC2 java framework
Contact Information

Paulo Asterio de Castro Guerra
asterio@ic.unicamp.br

Cecília Mary F. Rubira
cmrubira@ic.unicamp.br

Rogério de Lemos
r.delemos@ukc.ac.uk
Implementation Issues

Asynchronicity
Implicit Invocation
Multiple notifications
Asynchronicity

Service Request

Synchronous channels with higher priority
Implicit Invocation

iC2C_top

NormalActivity

iC2C_internal

AbnormalActivity

iC2C_bottom

Notification with i.i.

Mutual exclusion protocol

Service Request
Multiple Notifications

- BasicNormal
  - Stores notifications

- Collaborating Component
  - Evaluates post-condition

- normal_top

- normal_bottom