

Workshop on Architecting Dependable Systems
Orlando, FL – May, 25th 2002

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

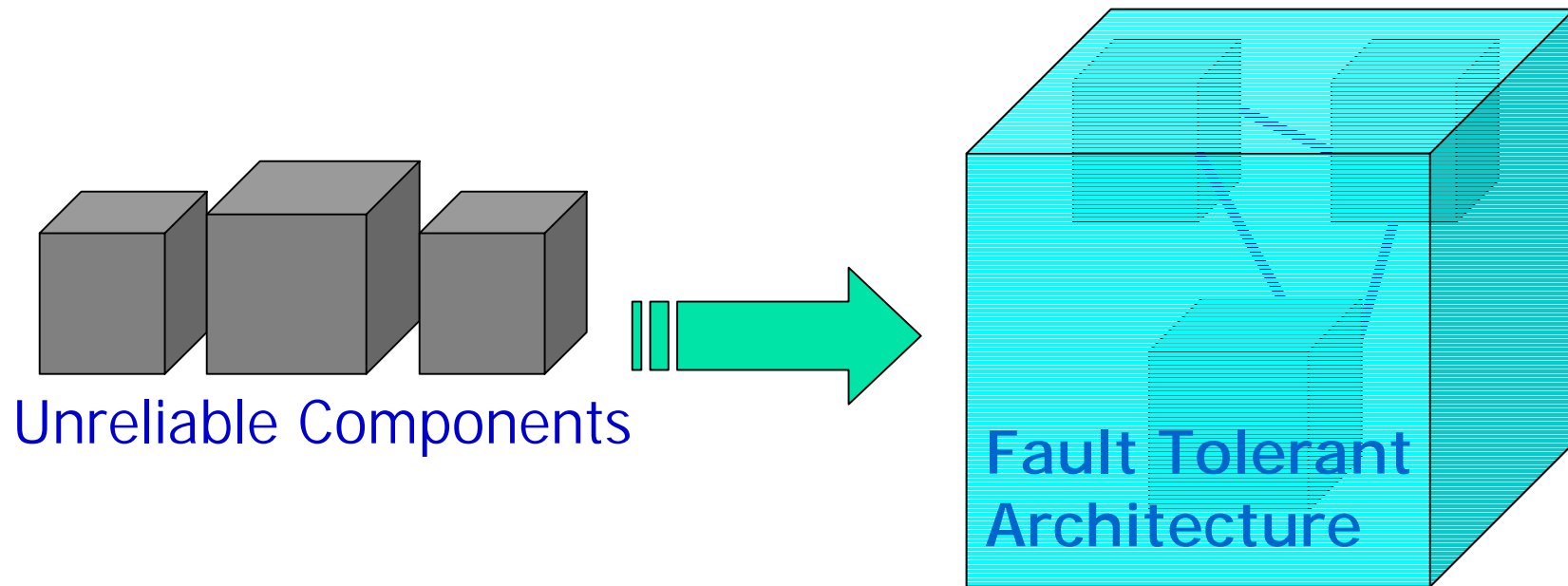
Computing Laboratory

University of Kent at Canterbury, UK



Motivation

- Reliable Component-Based Systems

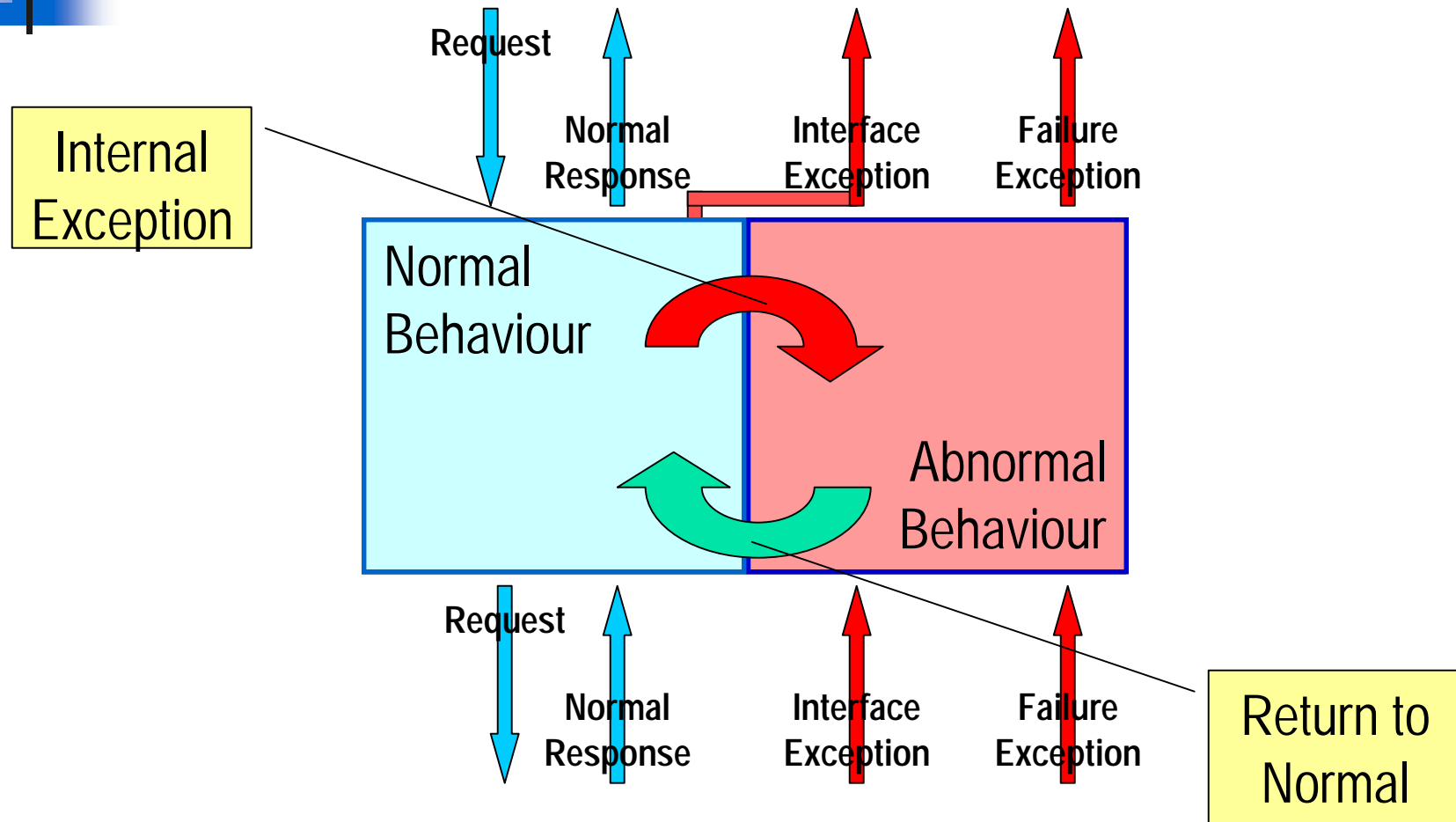




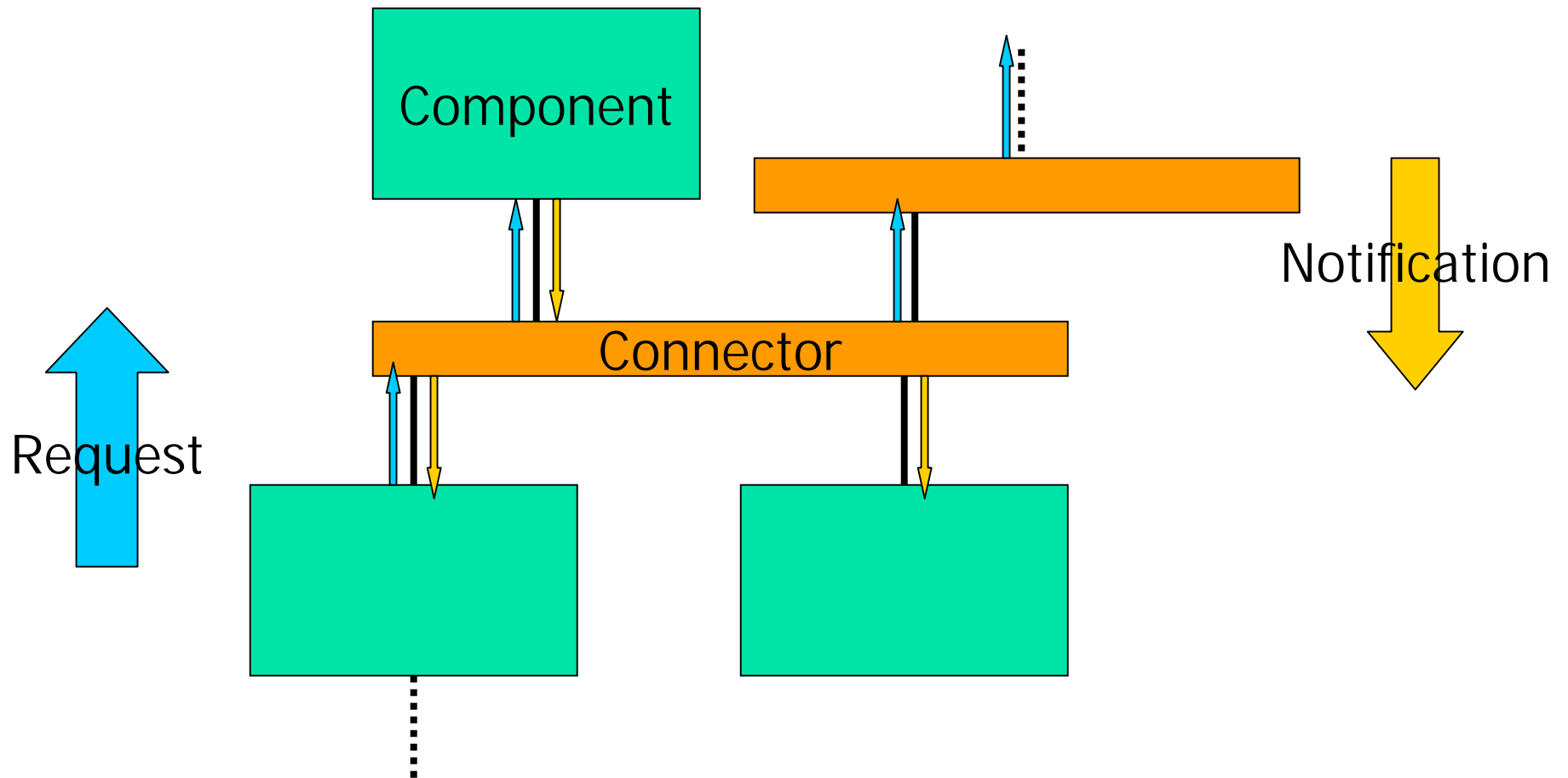
Objectives

- 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



The C2 Architectural Style

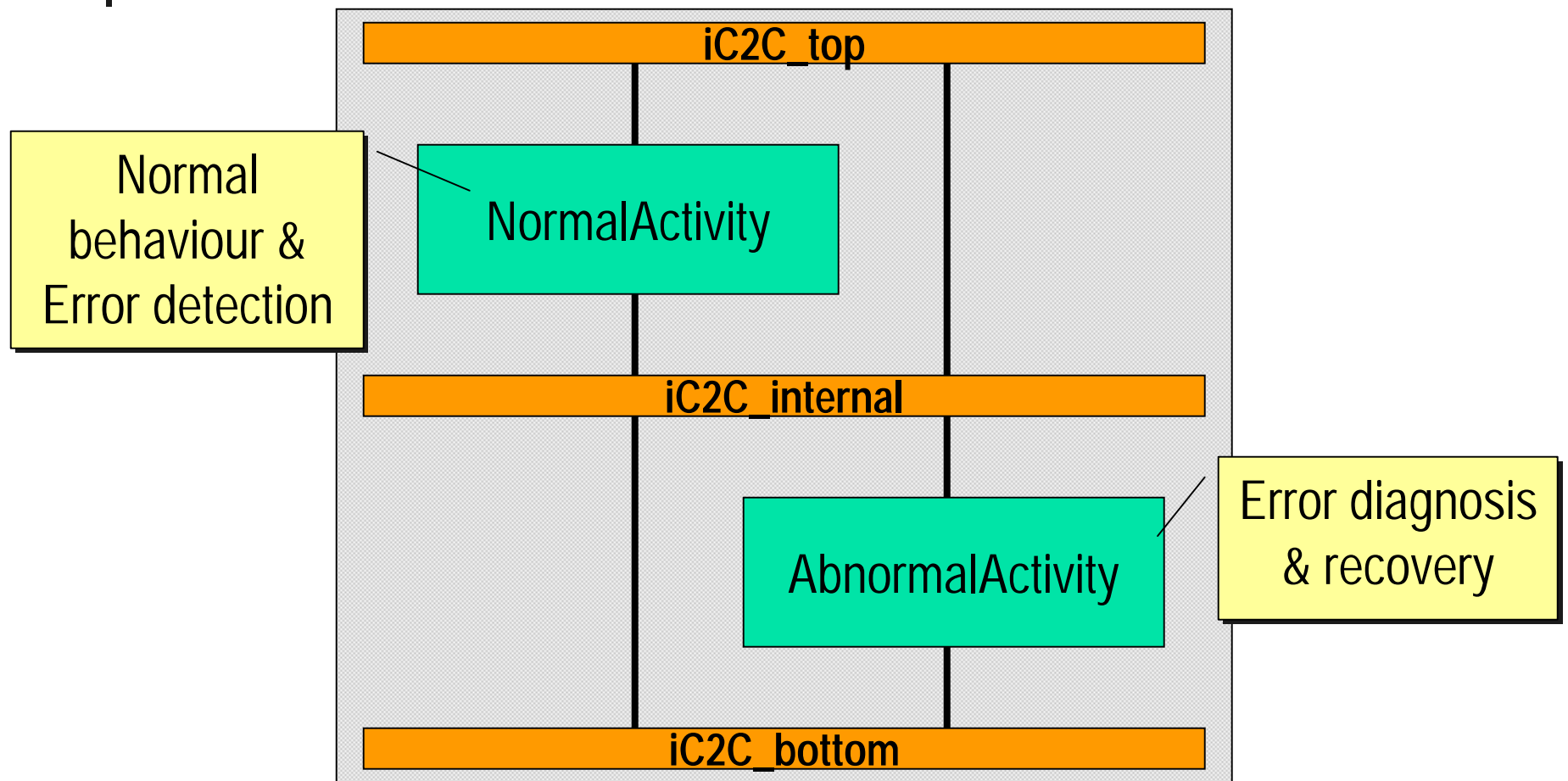




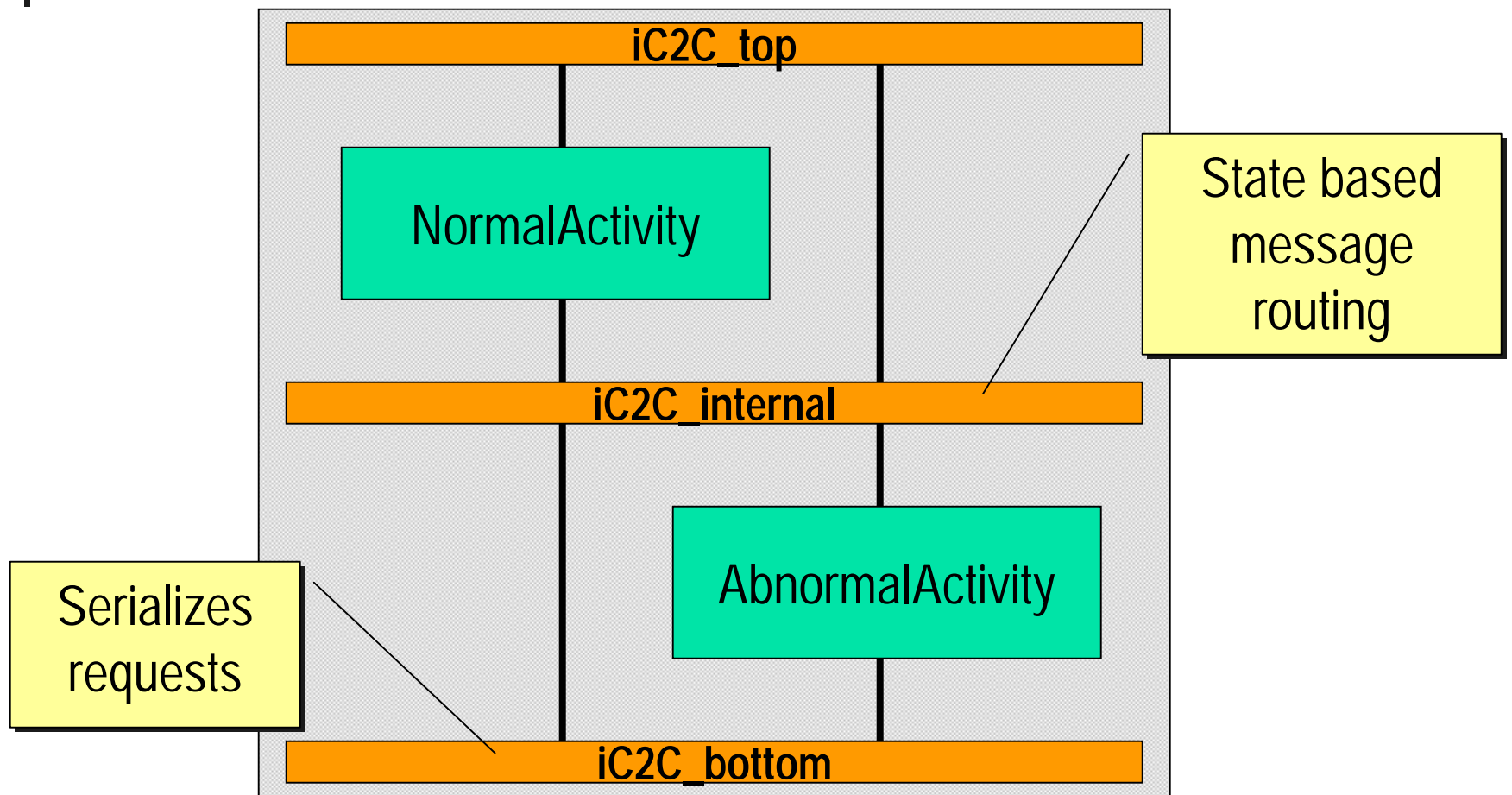
Proposed Architecture

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

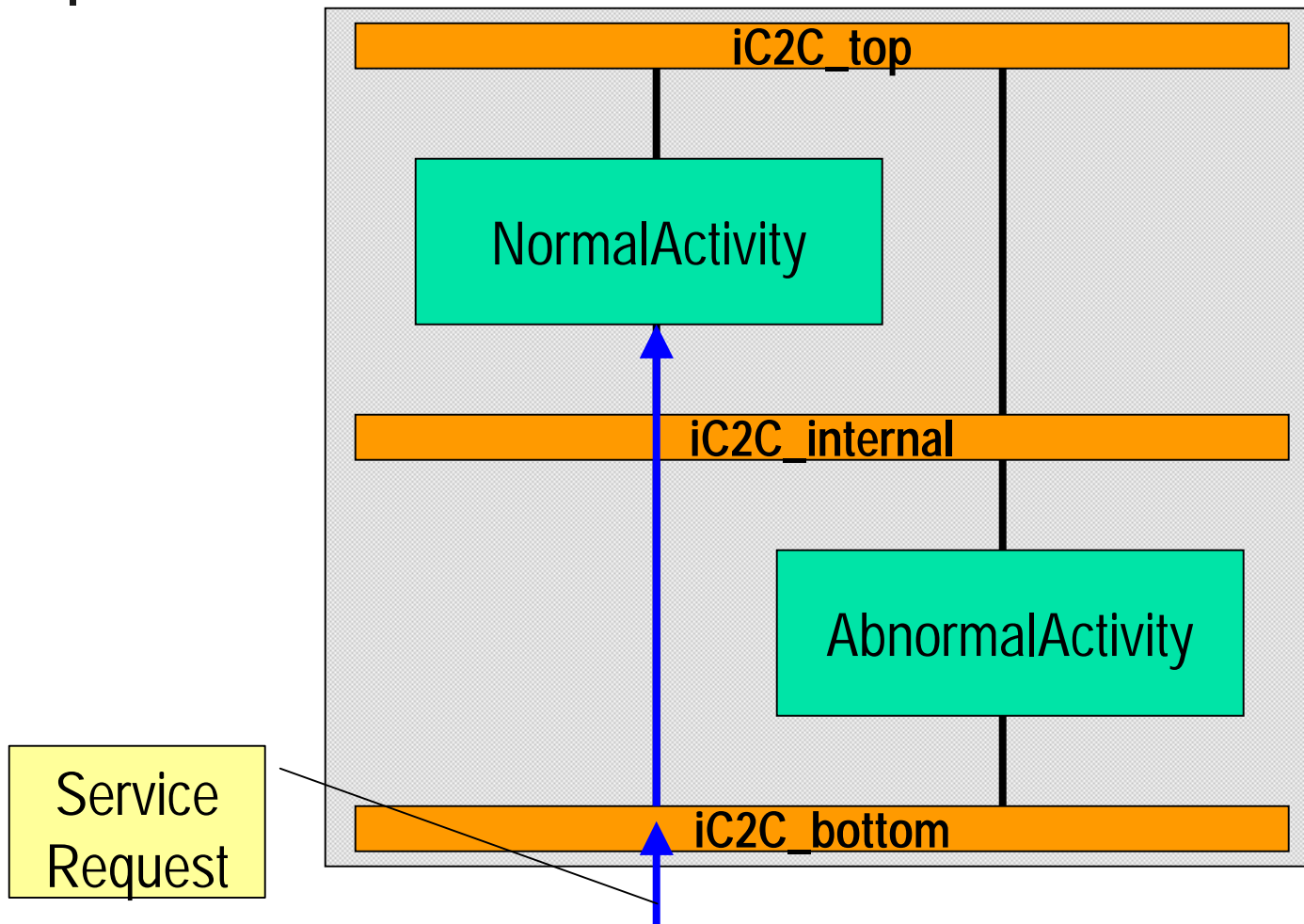
Overall Structure



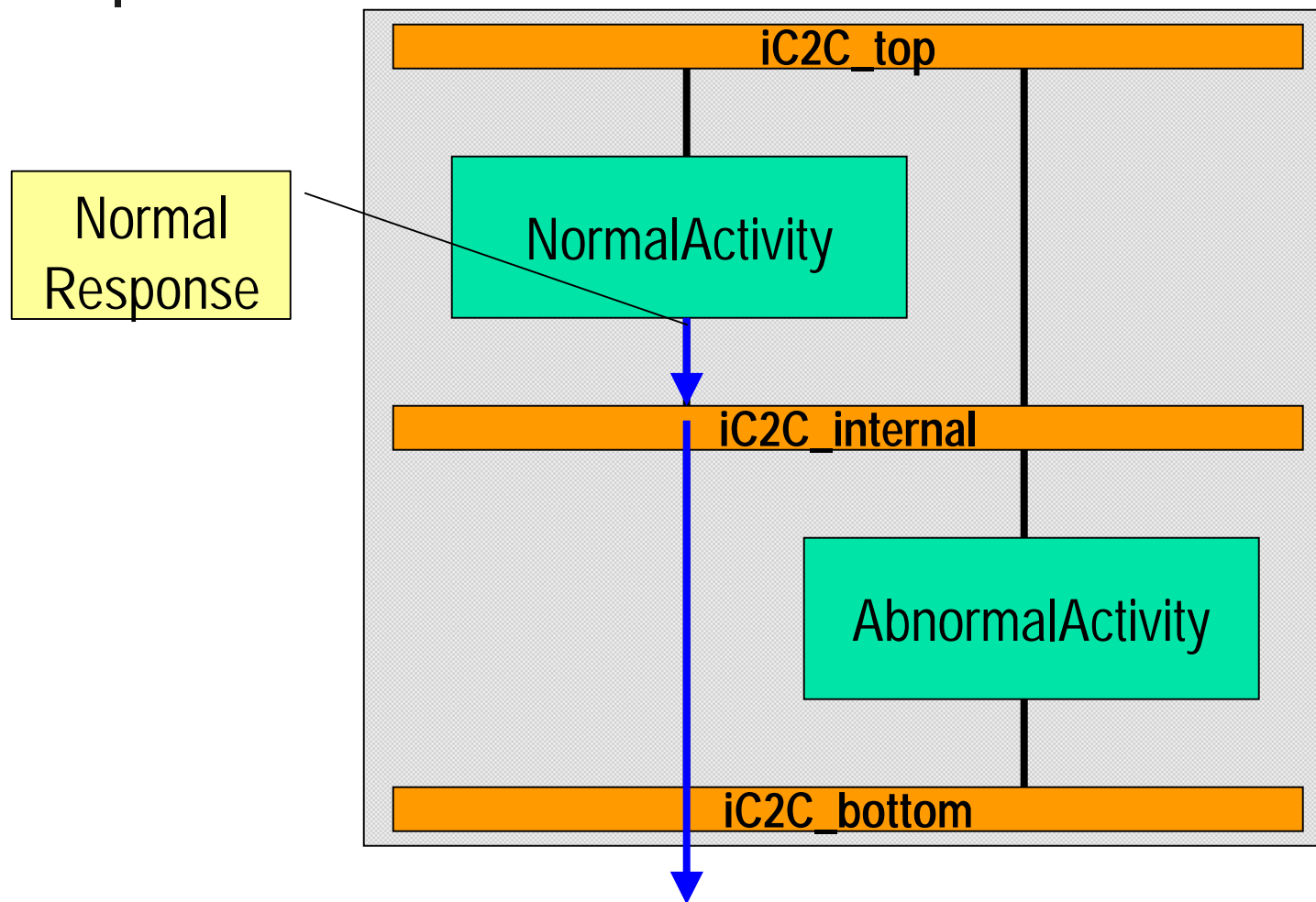
Overall Structure



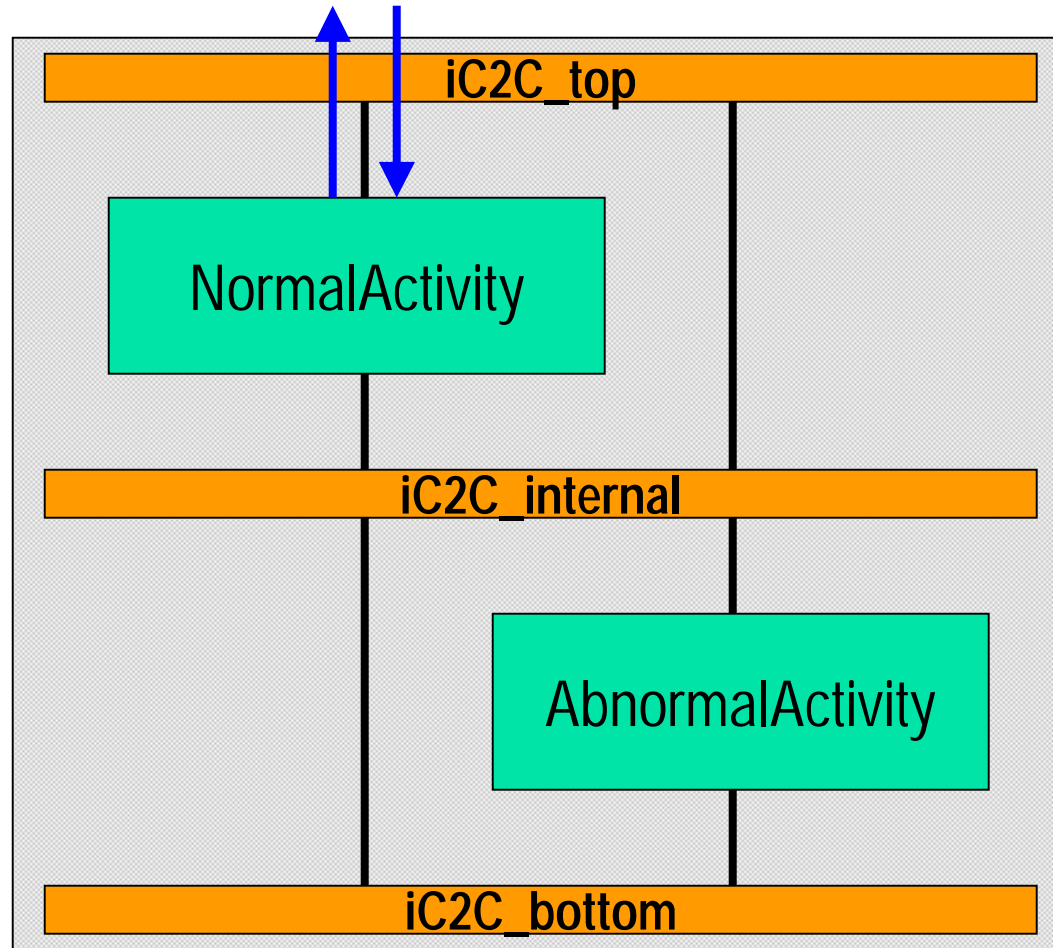
Normal Message Flow



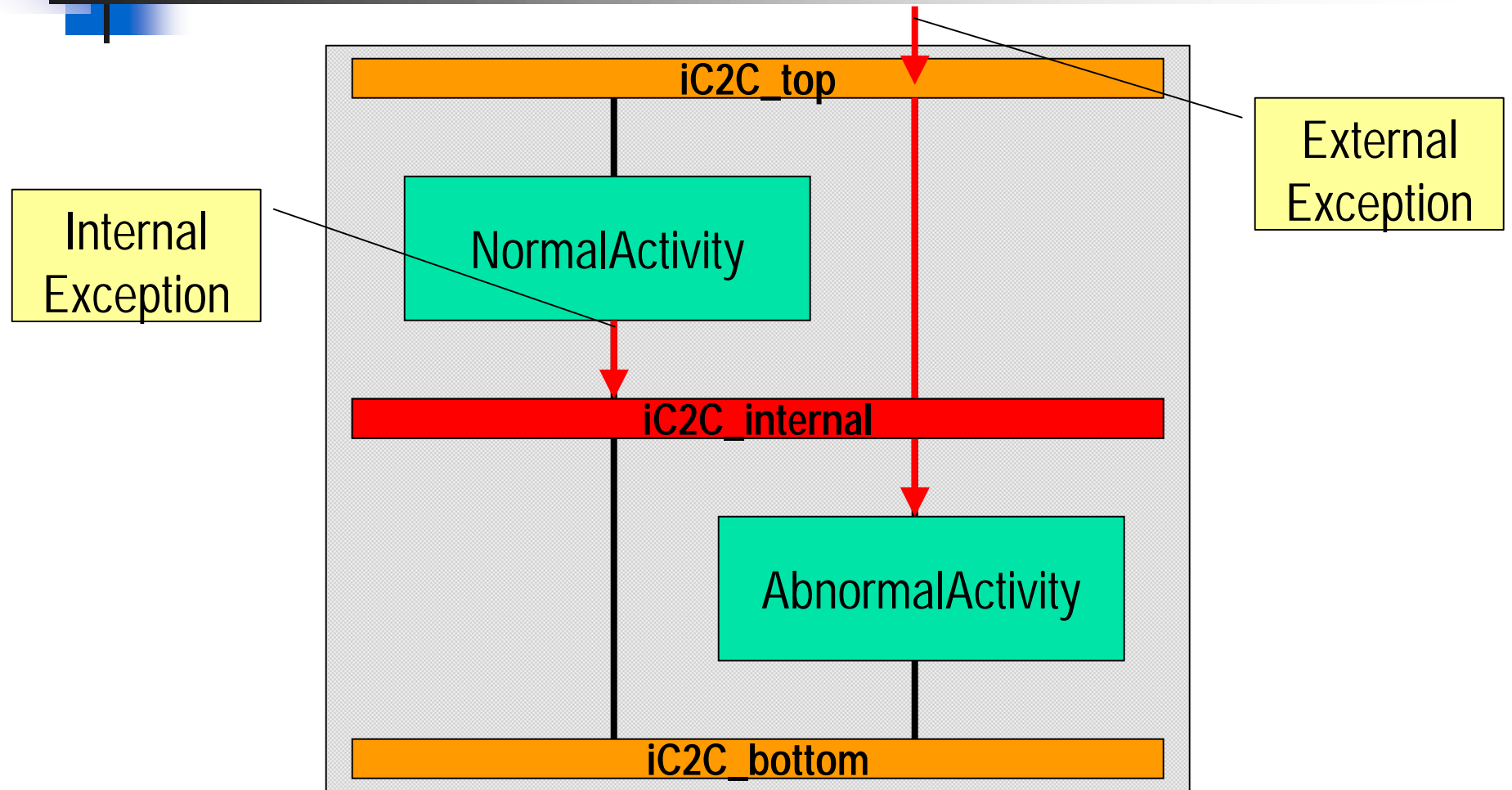
Normal Message Flow



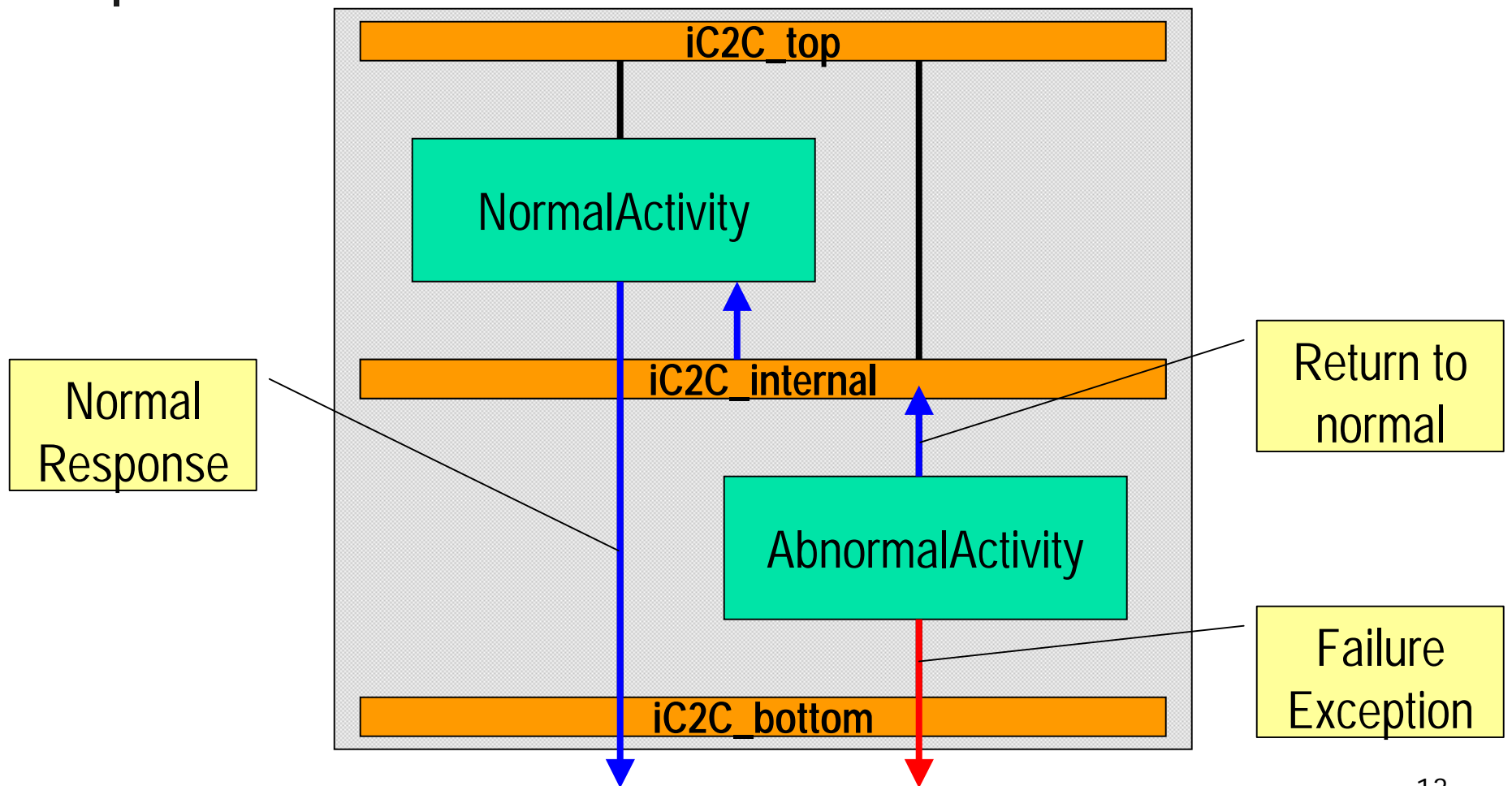
Normal Message Flow



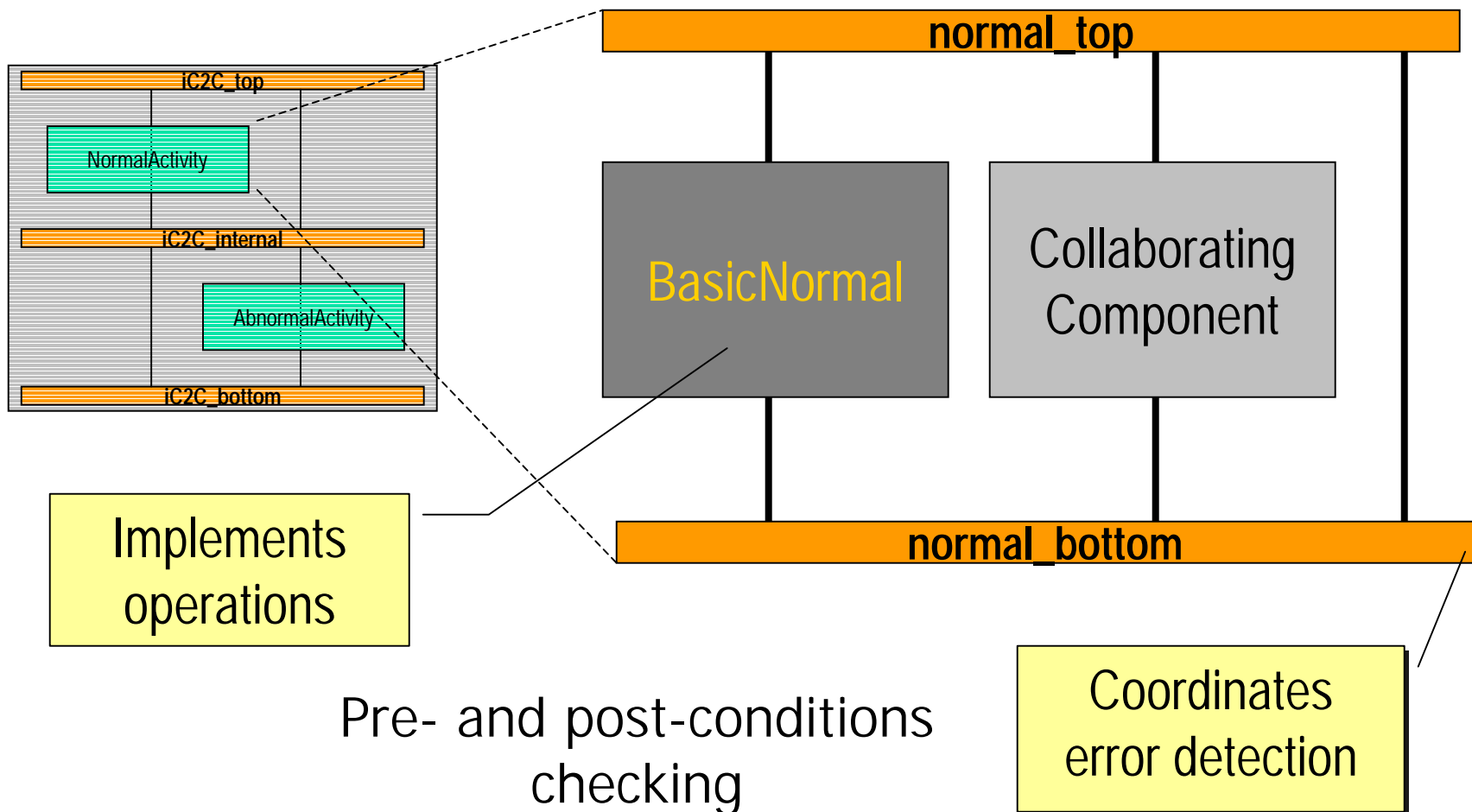
Abnormal Message Flow



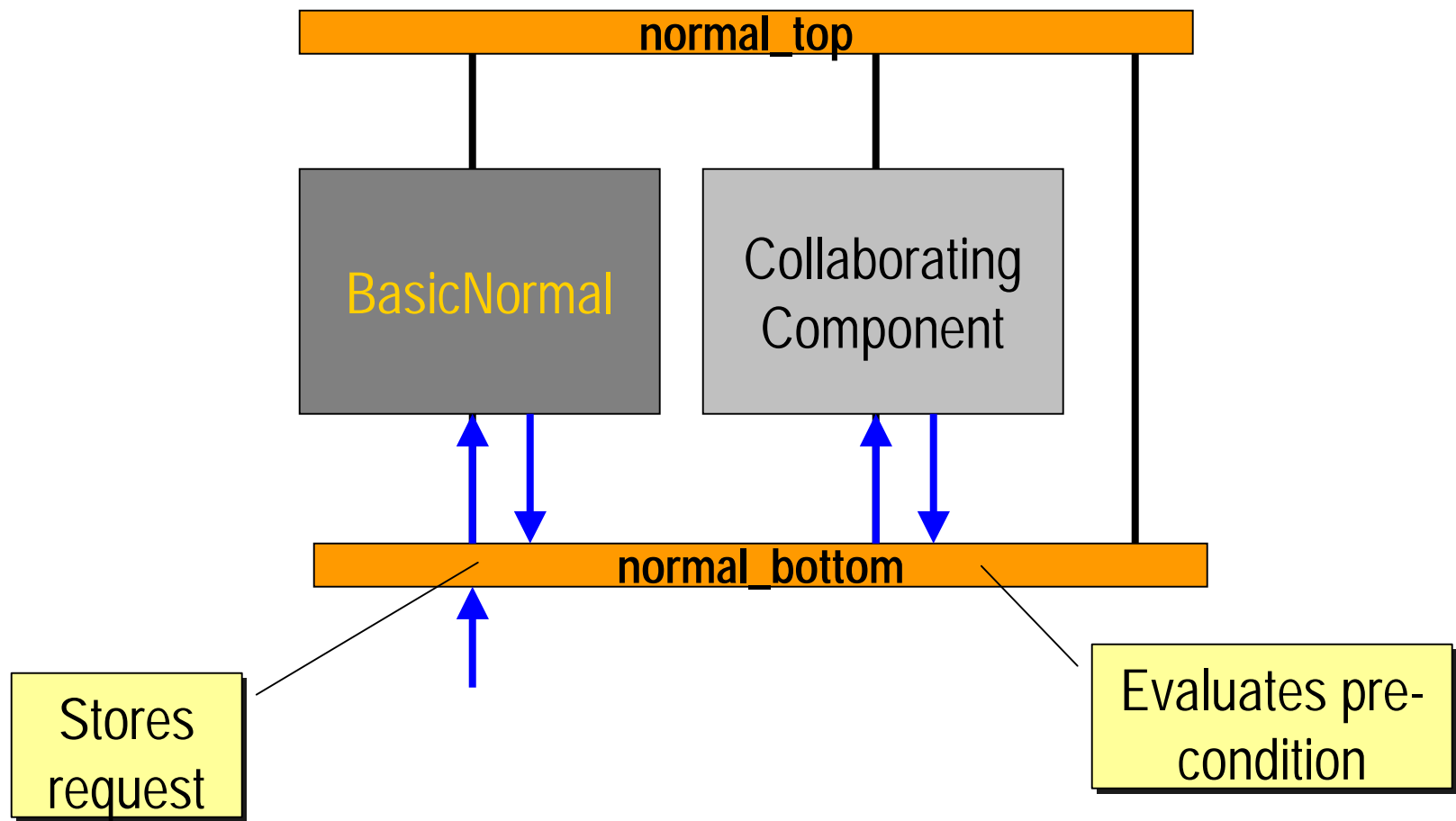
Abnormal Message Flow



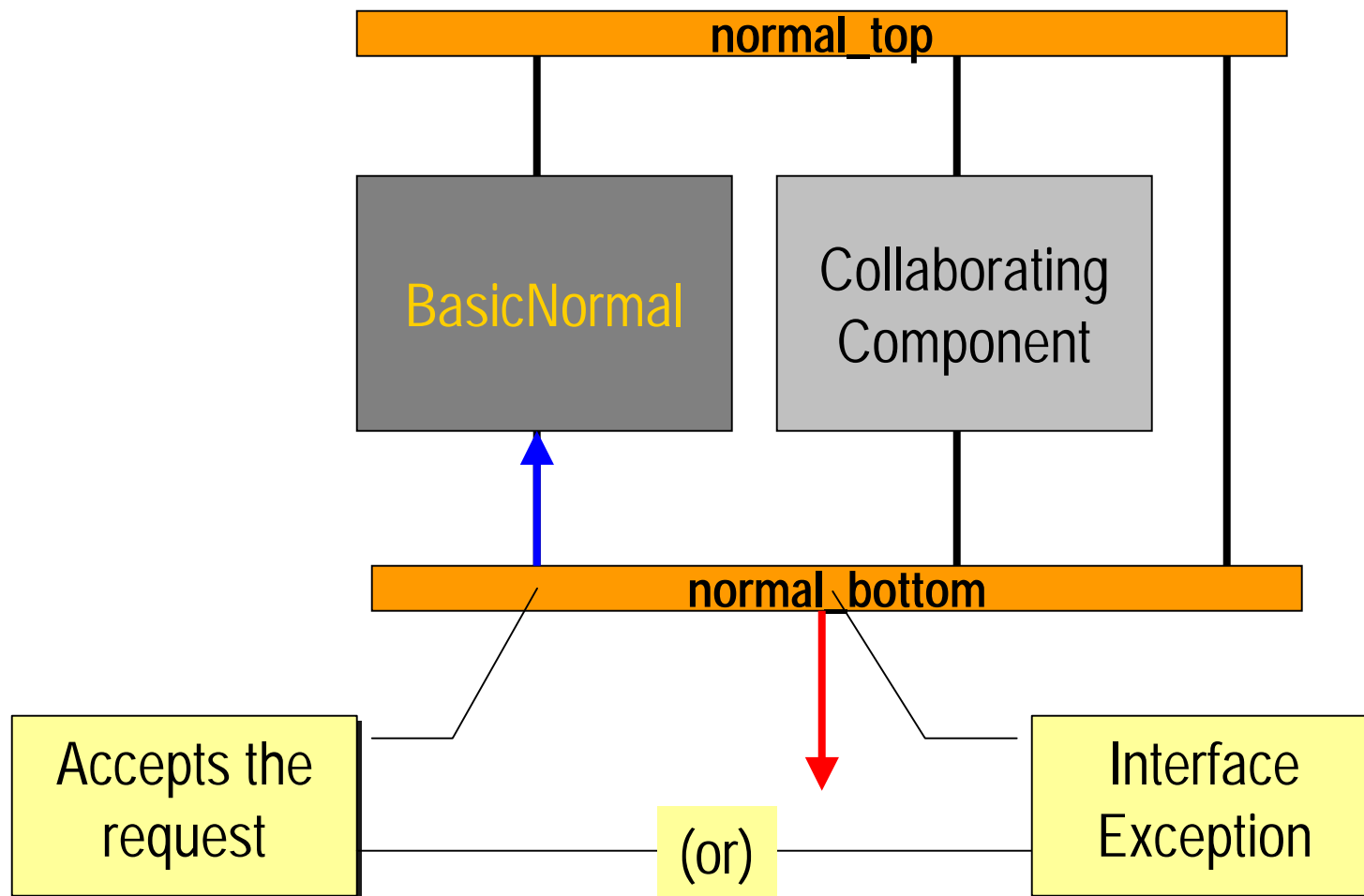
The NormalActivity Component



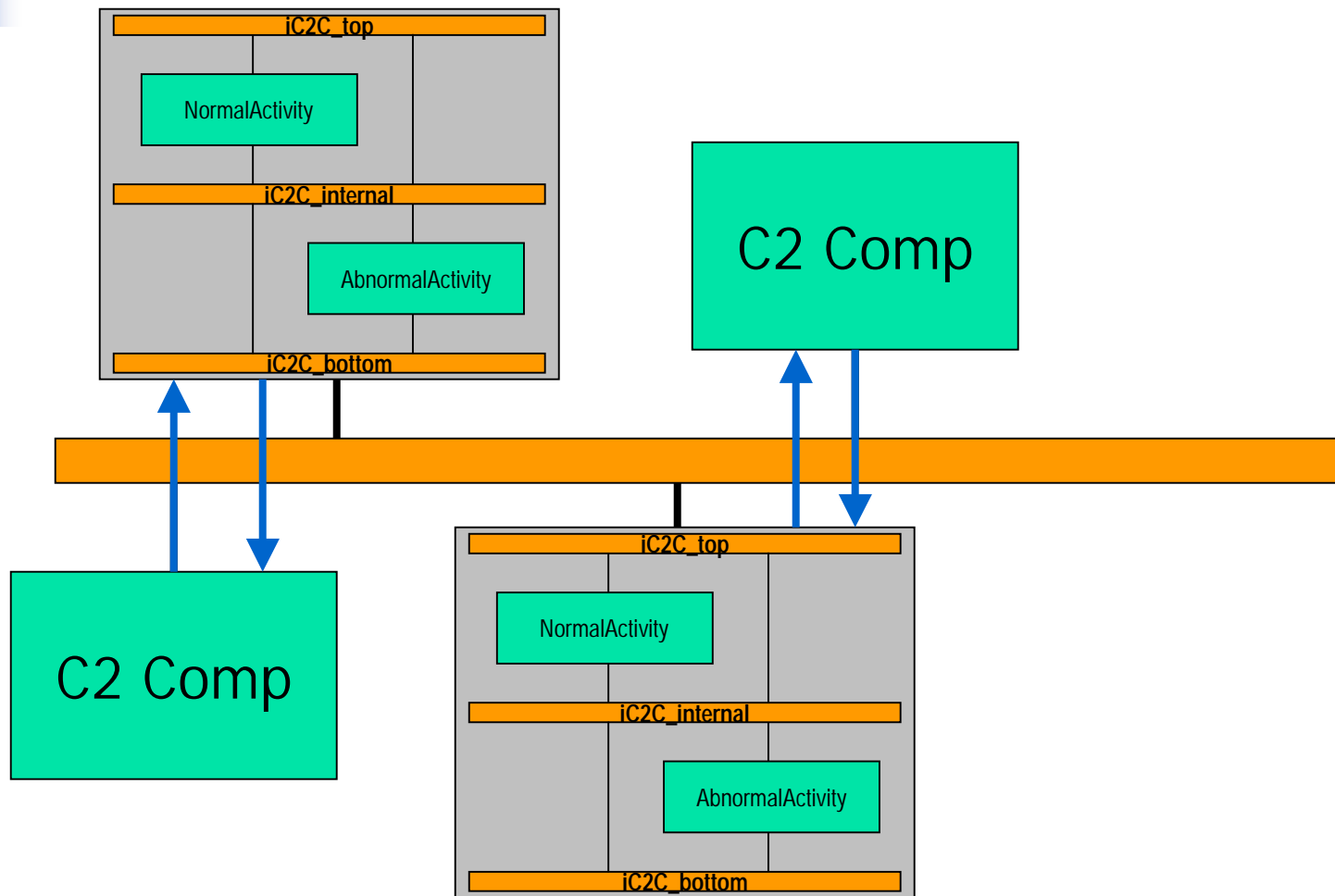
The NormalActivity Component



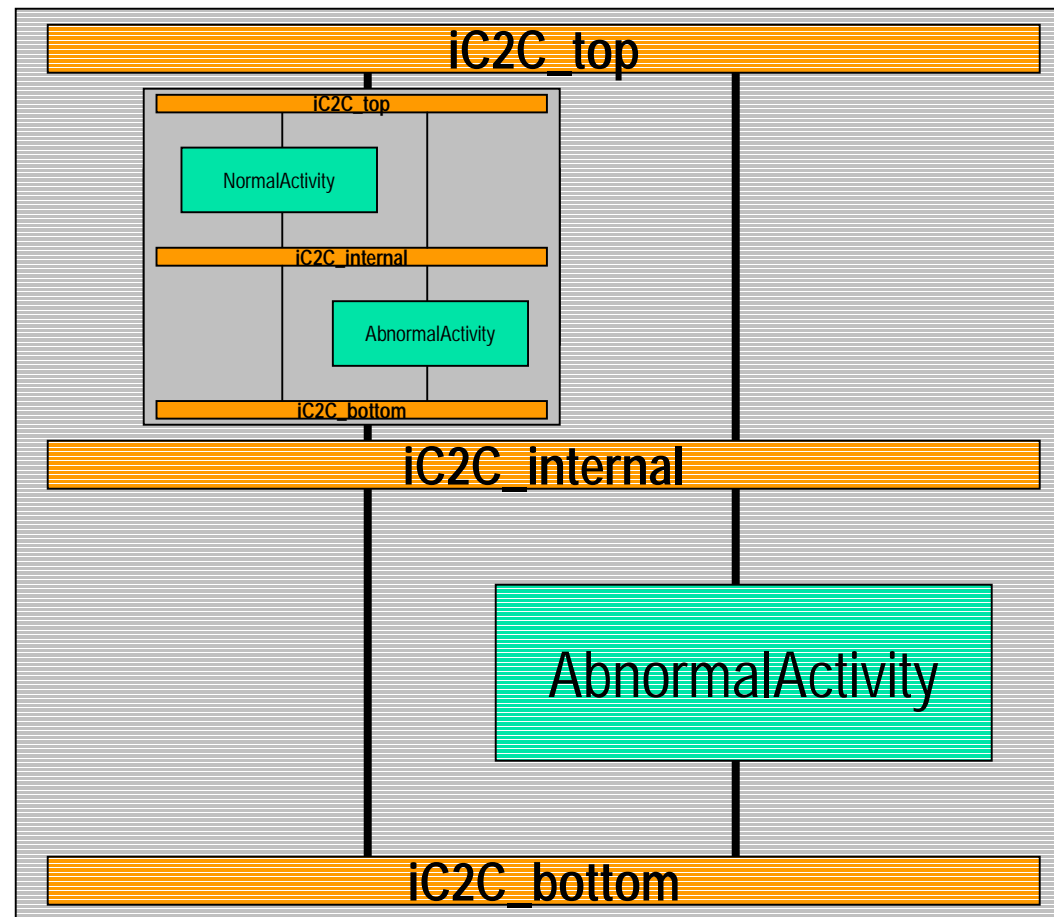
The NormalActivity Component



C2 Integration



C2 Integration

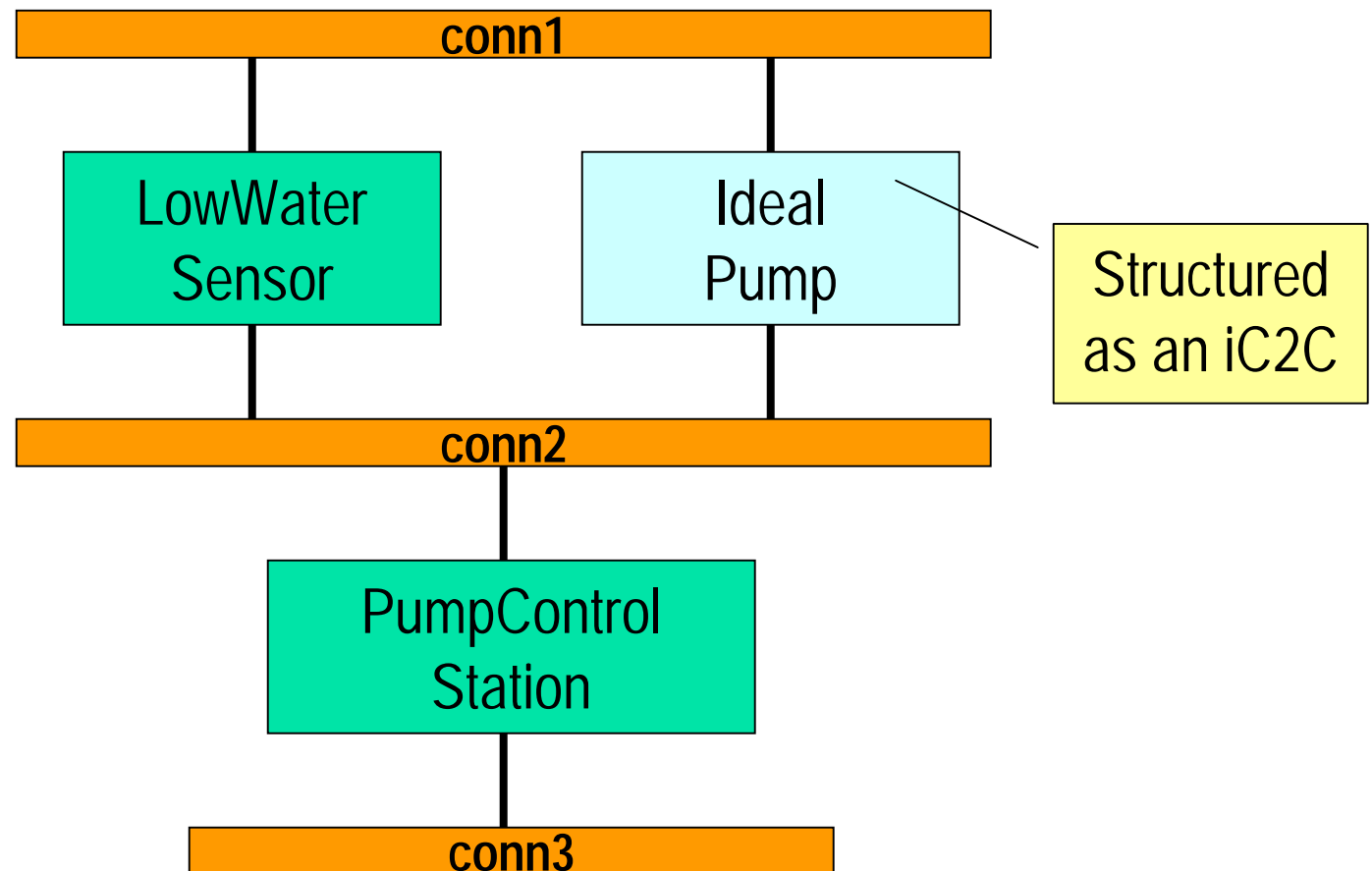




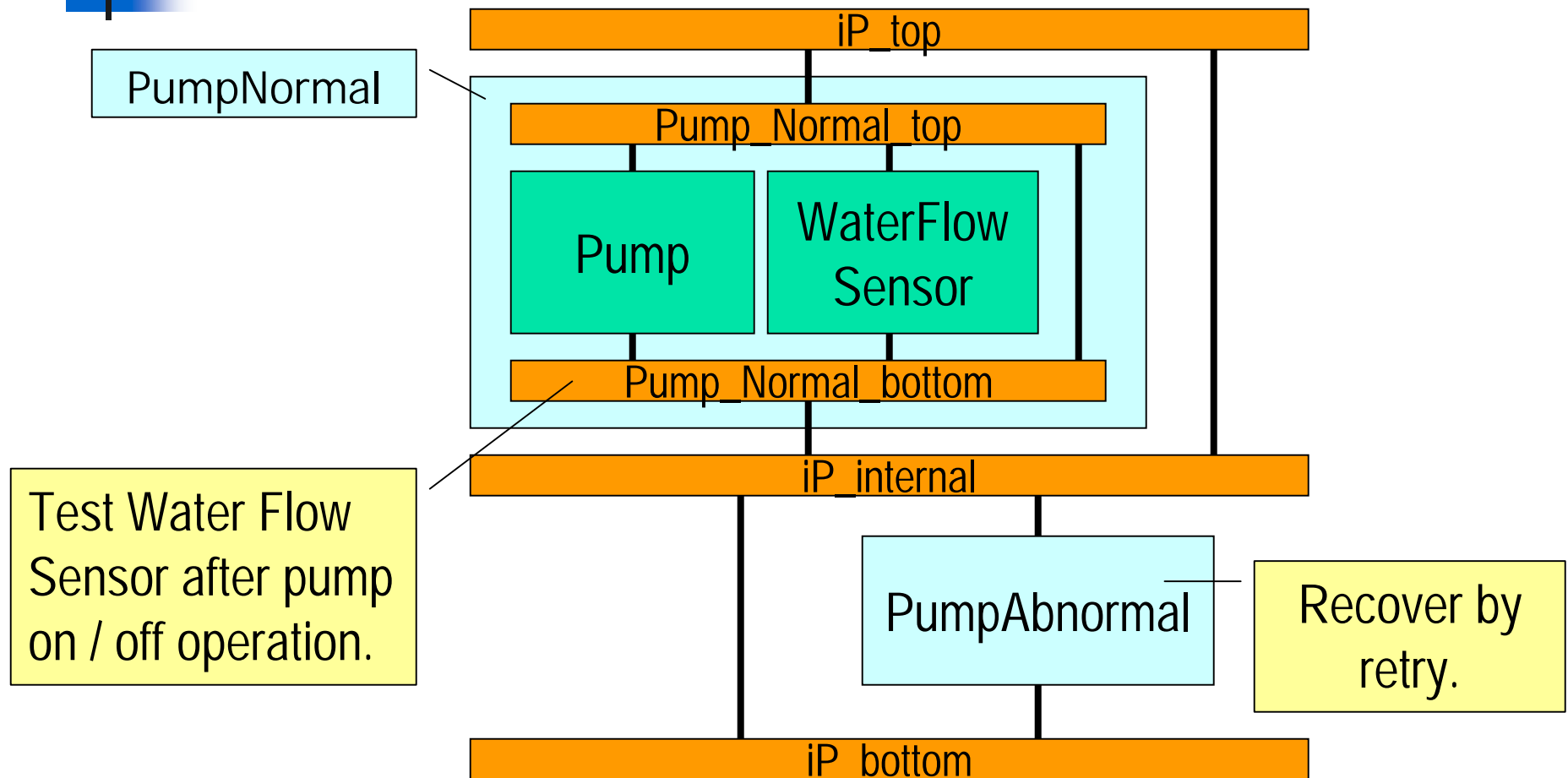
Example – Mine Pump Control System

- Fault Model
 - Transient faults affecting pump
- Error Detection
 - Test water flow sensor (reliable)
- Error Recovery
 - Retry operation

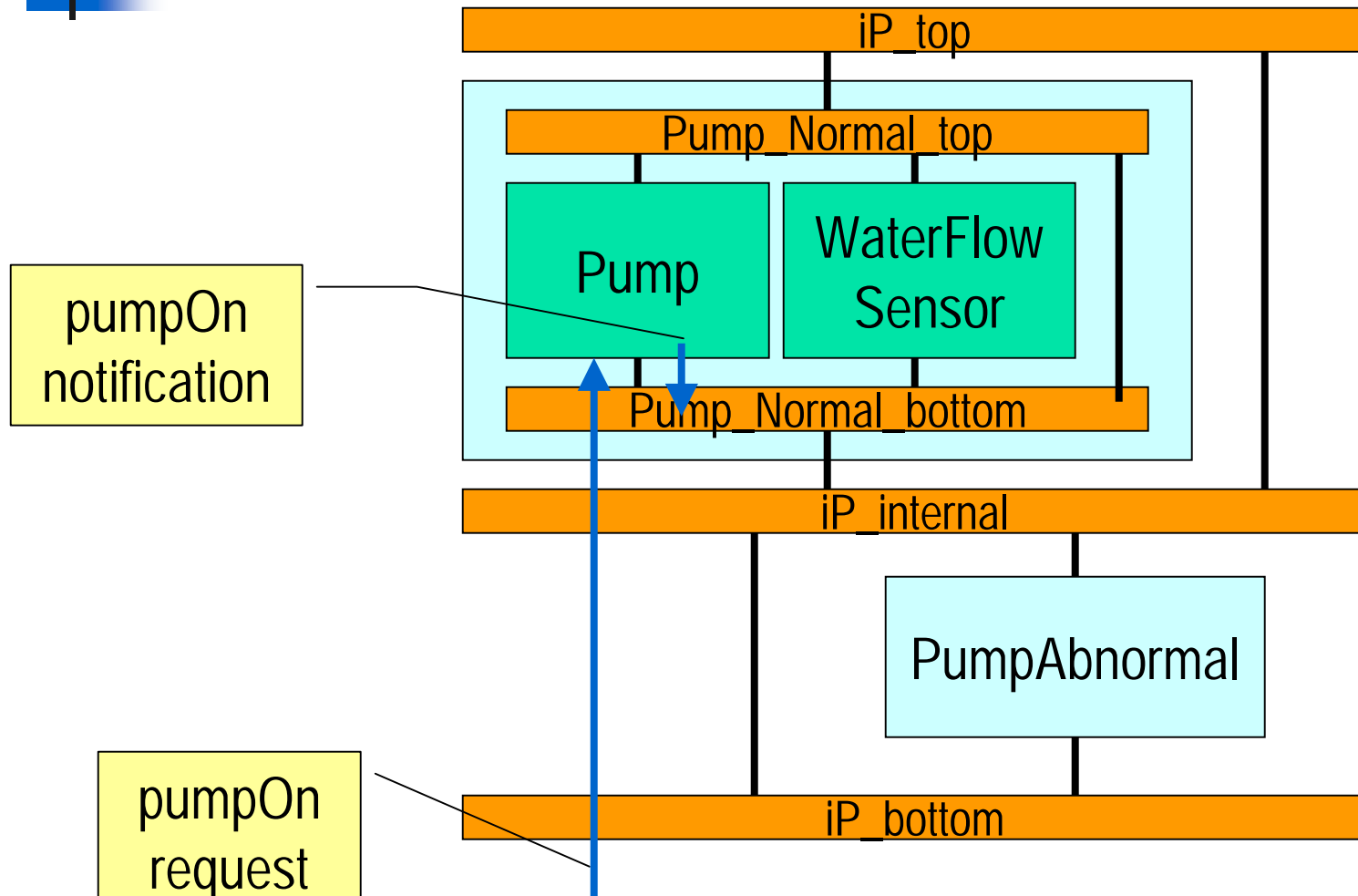
Subsystem Configuration



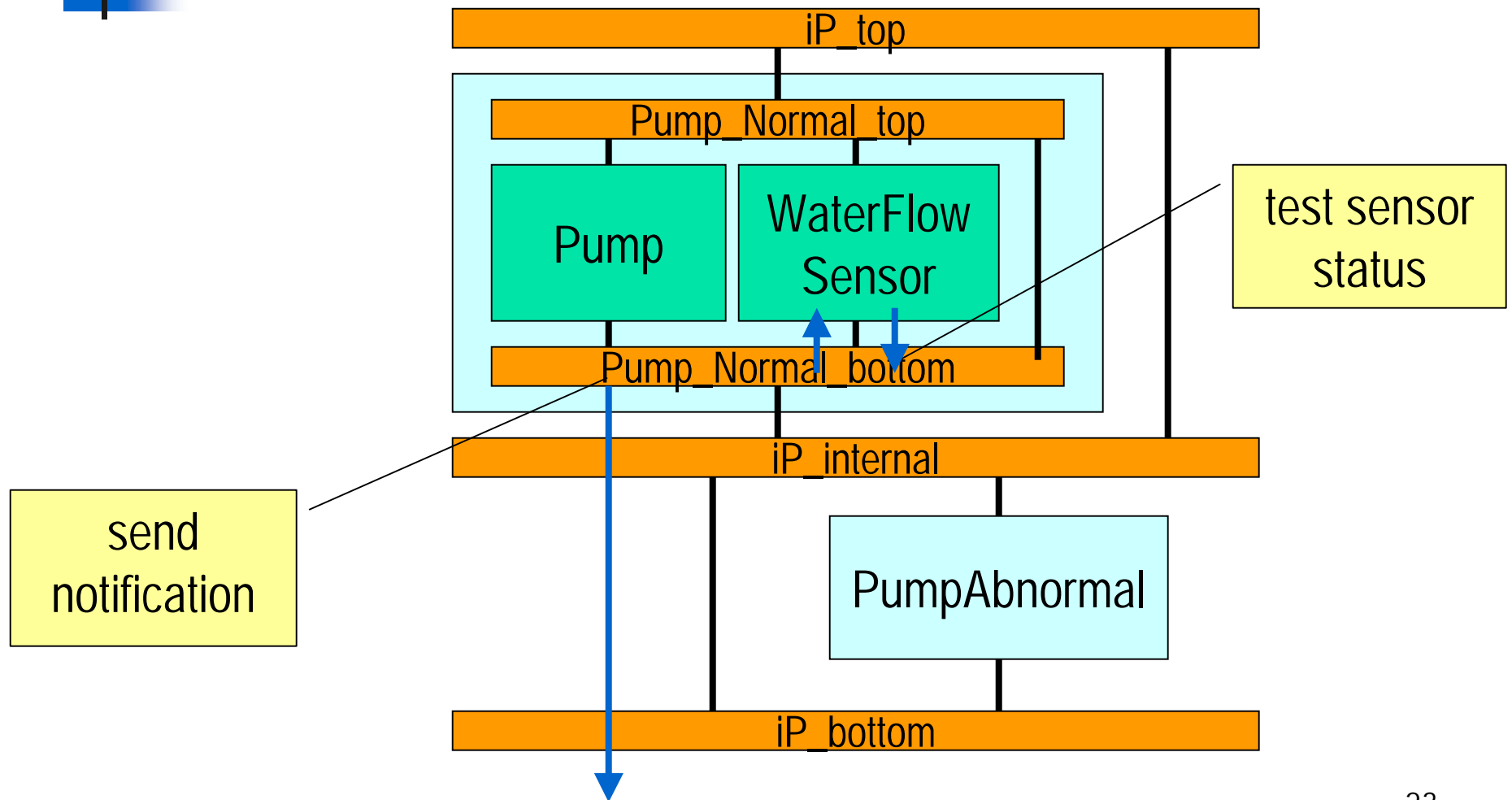
Ideal Pump Structure



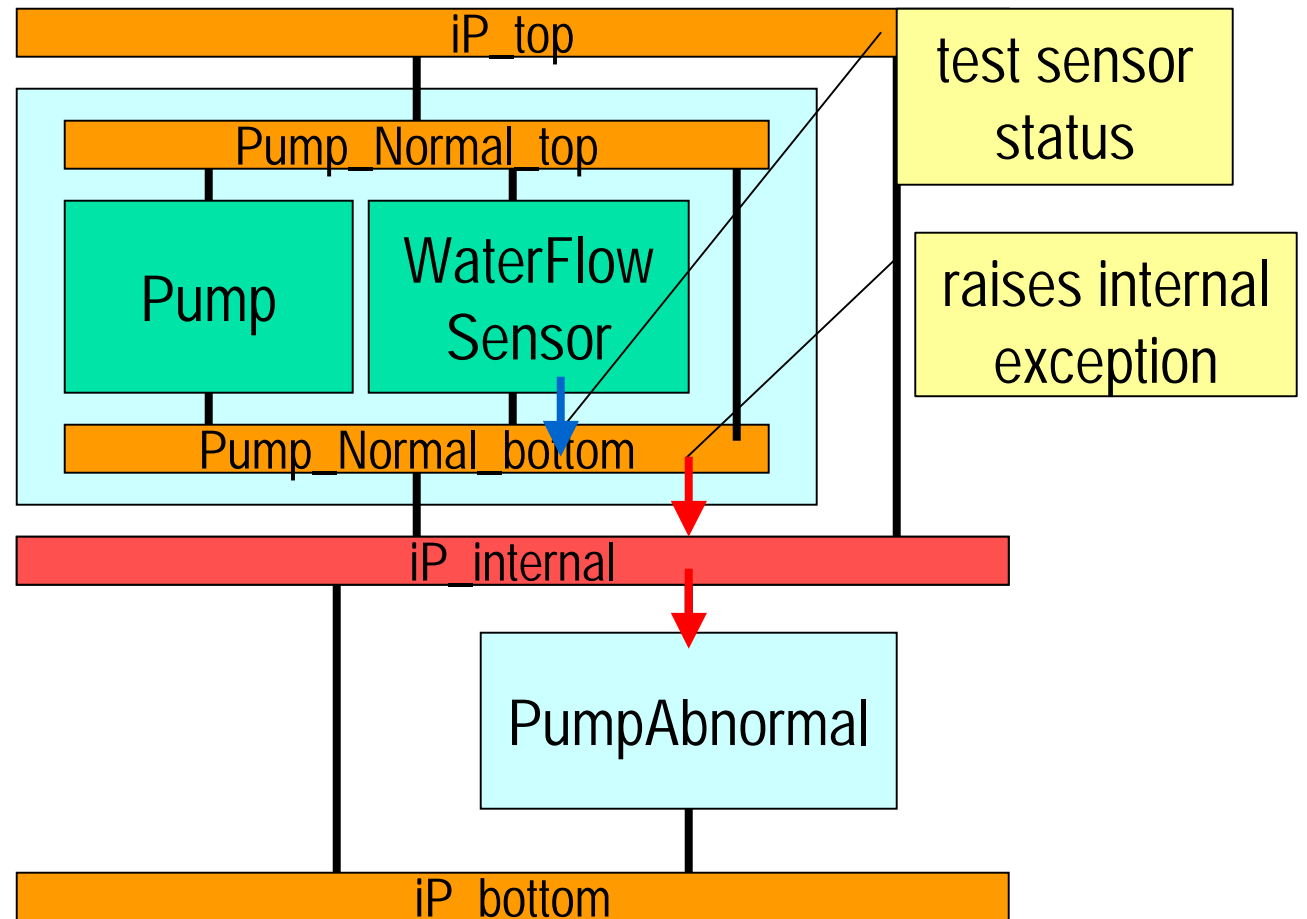
Normal pumpOn



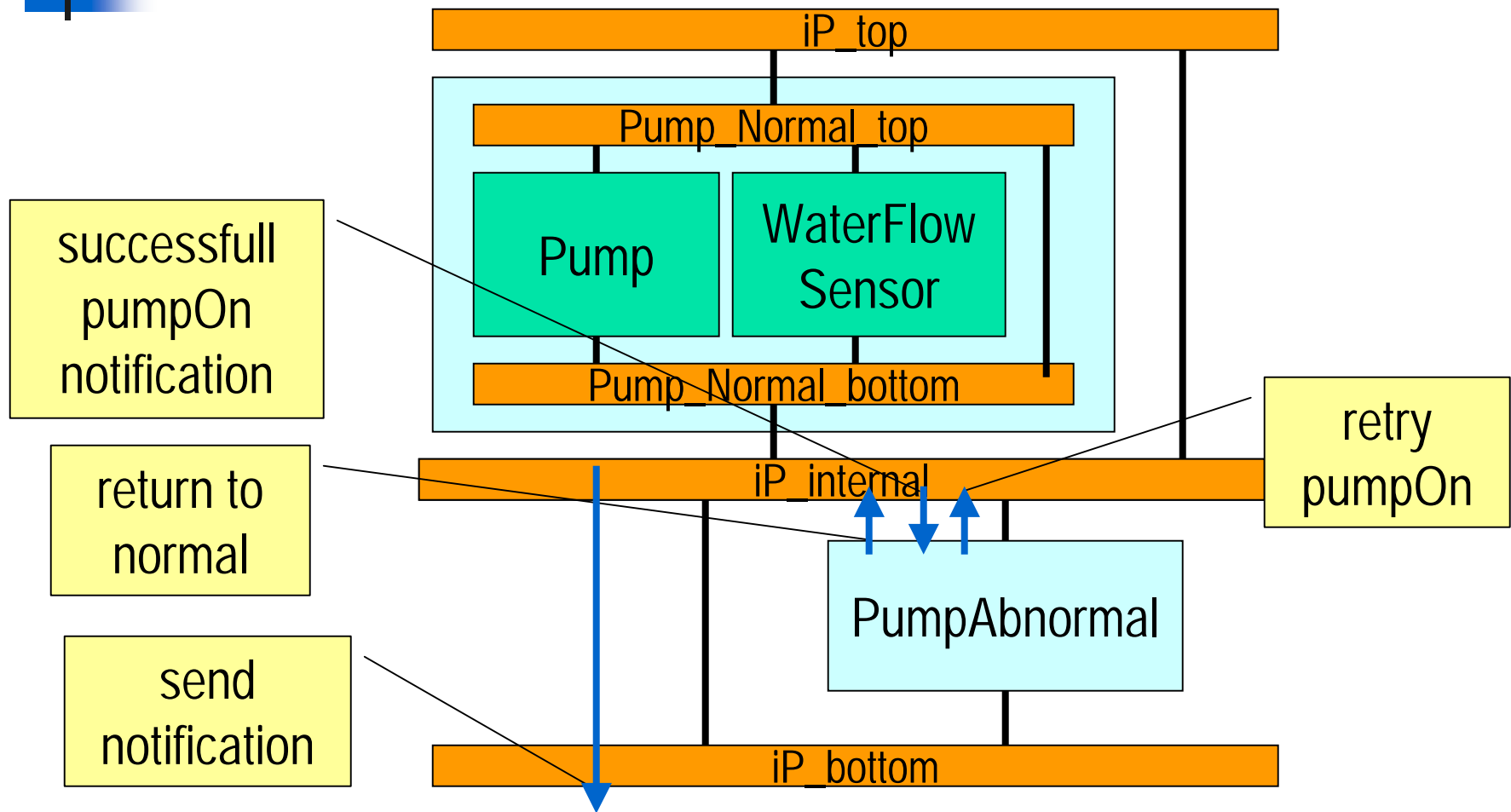
Normal pumpOn



Error Detection



Error Recovery





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



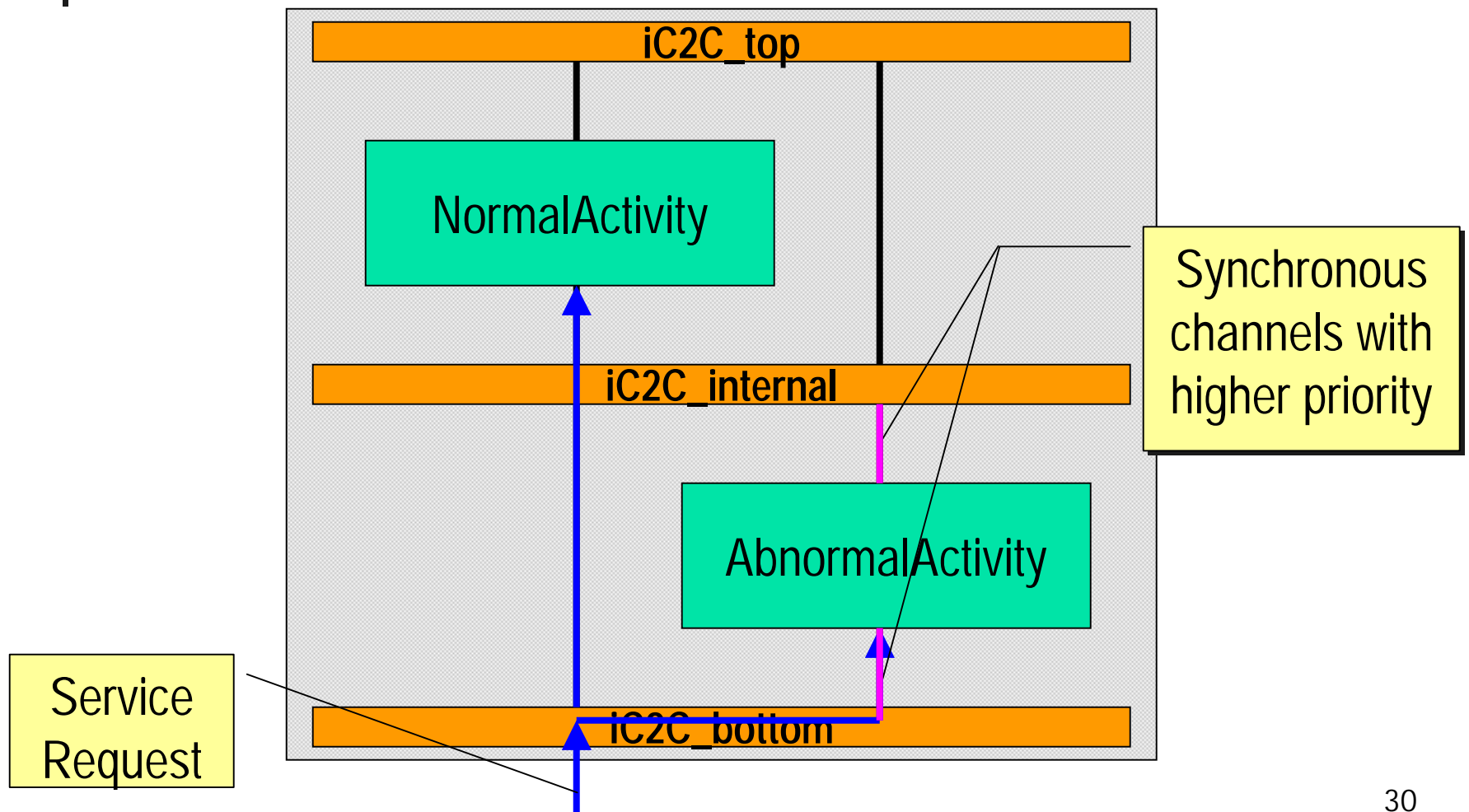
Implementation Issues

Asynchronicity

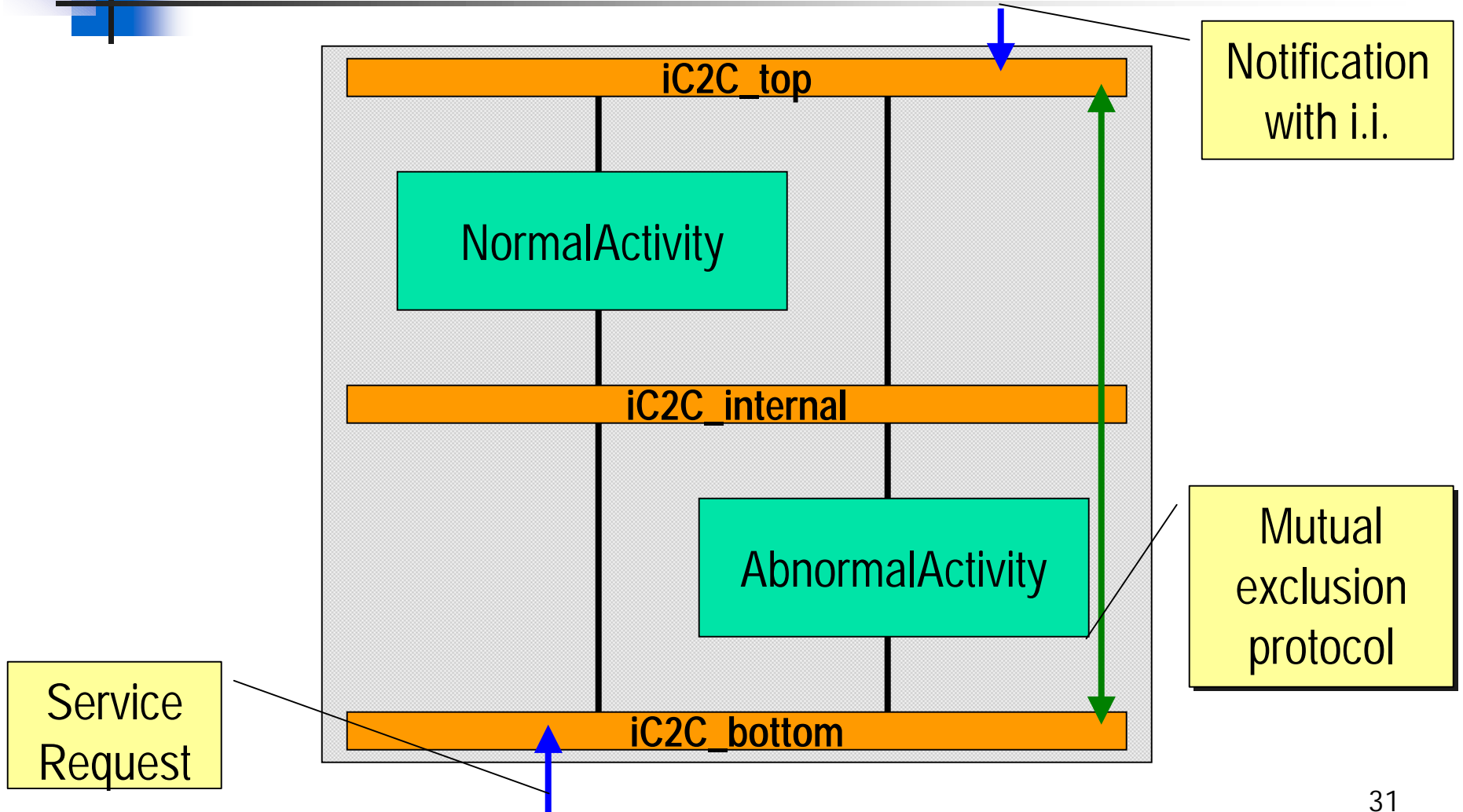
Implicit Invocation

Multiple notifications

Asynchronicity



Implicit Invocation



Multiple Notifications

