Overview of CORBA Fault Tolerance for TAO

Balachandran Natarajan
bala@cs.wustl.edu
http://www.cs.wustl.edu/~bala/
Advisor: Dr. Douglas C. Schmidt

November 17, 1999

Problem: How to Manage Failures in TAO?

- Harmful effects of failures on mission-critical applications
- Some common failures include
  – Network failure, Host, OS
  – Process, Object
- Application developers can attempt to solve the problem
- Application-level solutions are-error prone, non-reusable and, inflexible
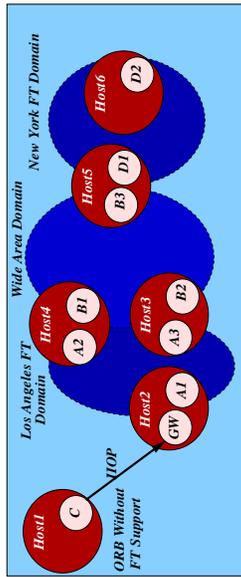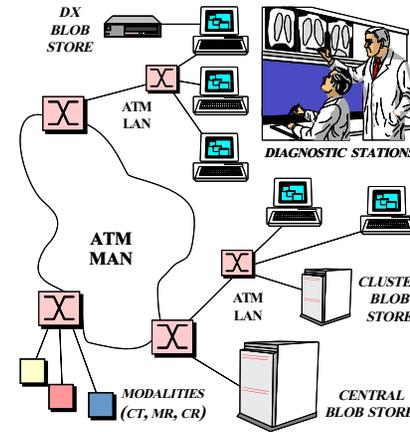

Solution: CORBA Fault Tolerant (FT) Spec

www.omg.org/techprocess/meetings/schedule/Fault_Tolerance_RFP.html

- Addresses common problems at the middleware level
- Fault tolerance is transparent the applications
- Provide customizable & reusable components for
  – Fault Detection
  – Fault Containment
  – Fault Masking
  – Fault Compensation
  – Fault Repair
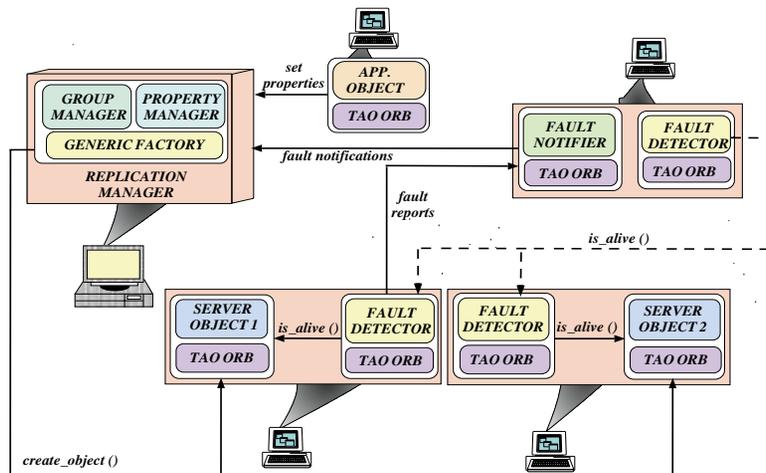
Washington University

Overview of FT Spec Features

- FT spec addresses the following issues
  – Fault tolerance through redundancy management
  – Eliminating single points of failure
  – Providing a range of Strategies
  – Minimize modifications to application code
  – Replication & fault transparency to the client

- The new concepts added to the CORBA model to provide FT are
  – Replication and grouping
  – Identification of domains
  – Properties for the domain
  – Domain consistency specification

Overview of FT Scenario

set properties

GROUP MANAGER | PROPERTY MANAGER
GENERIC FACTORY
REPLICATION MANAGER

APP. OBJECT
TAO ORB

FAULT NOTIFIER | FAULT DETECTOR
TAO ORB | TAO ORB

fault notifications

fault reports

is_alive ()

SERVER OBJECT 1 | is_alive () | FAULT DETECTOR
TAO ORB | TAO ORB

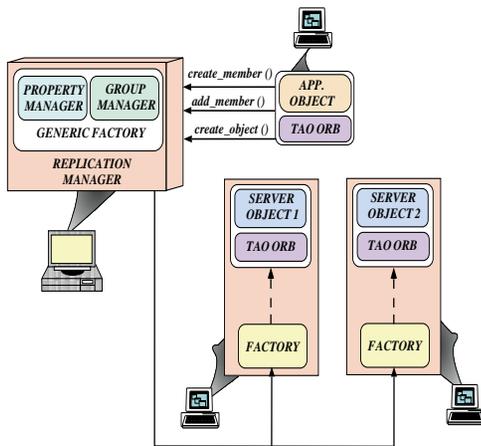FAULT DETECTOR | is_alive () | SERVER OBJECT 2
TAO ORB | TAO ORB

create_object ()

FT Service Components

- Replication Manager
  - At least one per-domain
  - Heart of the FT spec
  - All the other components interact with the Replica Manager
  - Inherits the interface of `PropertyManager`, `ObjectGroupManager` and the `GenericFactory`

- Fault Detectors
  - Monitors objects using a "pull" monitoring interface
  - Numbers and arrangement are not restricted

- Fault Notifiers

- Logging and Recovery Managers

Replication Manager

PROPERTY MANAGER | GROUP MANAGER
GENERIC FACTORY
REPLICATION MANAGER

create_member ()
add_member ()
create_object ()

APP. OBJECT
TAO ORB

SERVER OBJECT 1 | SERVER OBJECT 2
TAO ORB | TAO ORB

FACTORY | FACTORY

- Property Manager provides methods to add, edit, query & delete

  - Replication style - Stateless, Cold, Warm, Active
  - Membership & Consistency sty - Application or Infrastructure
  - Fault monitoring style and granularity
  - Factory information
  - Initial and minimum number of replicas
  - Fault monitor interval
  - Check point interval

## Replication Manager (Contd..)

- Object Group Manager:
  - Add a member to the group
  - Remove a member from the group
  - Control the locations of members of the group
  - Obtain current reference of a group

- Generic Factory :
  - Creation of replicated object groups
  - Creation of replicas
  - Creation of unreplicated objects
  - Implemented by the applications
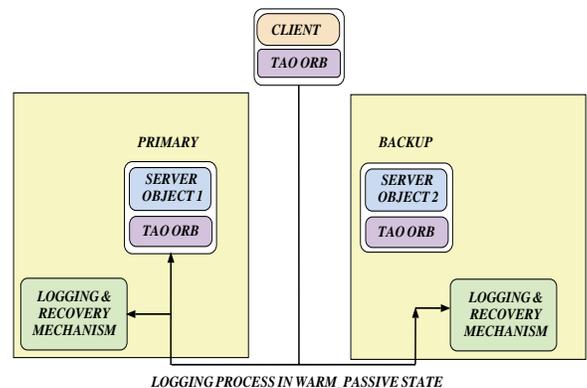
State Management (Contd..)

RECOVERY PROCESS IN WARM_PASSIVE STATE
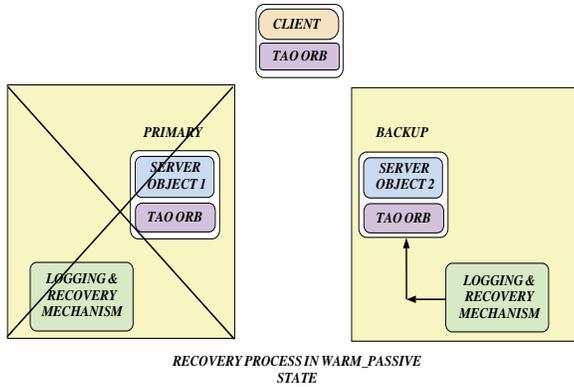
- The second stage is
  - Recovery after a fault
    * provides an interface for updation
    * journal is read to restore state
    * defined semantics for restoration based on replication style

---

Fault Management Components
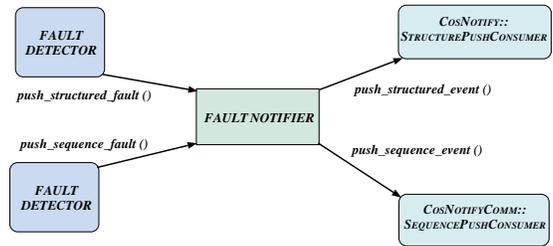
- Fault detectors
  - atleast one & usually more than 1
  - not shared across FT domains
  - monitors objects by providing a Pull based interface
- Fault notifier
  - interacts with detectors
  - gets reports from the detectors
  - filters reports
  - publishes reports to consumers
- Fault analyzer
  - application dependent

Changes in TAO to Support FT Spec

- TAG_ALTERNATE_IIOP_ADDRESS component needs to be used
- Addition of the following to the standard IOR components
  - TAG_GROUP, TAG_PRIMARY, TAG_HEARTBEAT_ENABLED
- Addition of service context
  - GROUP_VERSION, REQUEST
- Policy identifiers
- LocationForward/Object Forward
- An extended failover semantics
- Addition of FT service components

State Management

LOGGING PROCESS IN WARM_PASSIVE STATE

- The first stage is
  - Journaling or Logging during normal operations
    * provides an interface for check pointing
    * journals could be local or distributed
    * distributed logging necessitates a reliable totally-ordered multicast for recovery
    * journal management