Section 4: Design for Dependability-2

A. Bondavalli

Adding security to operational systems

Walter L. Heimerdinger

Dependability Challenges in Pushed-based Systems

Yennun Huang

High End Commercial Computer Fault Tolerance: Trends and Directions - AUTONOMIC COMPUTING

Lisa Spainhower

Adding security to operational systems

- ‘Classical’ dependability and security use a different sets of techniques often conflicting with each other
- The challenge is merging those techniques solving the various conflicts
  e.g. redundancy vs. confidentiality

Dependability challenges in Push-based distributed network applications

- Push: register somewhere to get some info and when it is available it will be sent automatically thus reducing the traffic over the internet
- Reliability challenges e.g.
  - Asynchronous Communications
  - Subscriber-based reliable broadcast
  - Exactly once delivery (filtered and dropped packets)
  - State replication and synchronization
- Scalability challenges e.g.
  - Large number of subscribers
  - Complex network management
- Security challenges e.g.
  - Content-based filtering and routing
  - management

Availability of real systems - Autonomic Computing

- **Availability of real systems** -- Several lessons learned:
  - **Good technology** and **Good management** are both needed
  - FT servers make a difference
  - Cluster difficult to implement
- Challenges
  - Firmware -- Circuit failure mechanisms -- State encapsulation -- On-the-fly changes -- Dynamic resources allocation -- Configuration validation
- **eLiza Project**: work in progress towards the 'perfect' system:
  - Self optimizing -- Automatic recovery -- Transparency
  - Interoperable services --- Dynamic selection -- ……..
- Should we build Autonomous systems to the extent that humans will not be needed anymore??
- Is it the case that automation simply removes 'less dangerous' failures and we remain with the most severe or does it "**Create**" new failures which could not occur before??