

## **Fault-tolerance in Distributed Real-Time Systems**

Farnam Jahanian  
Real-Time Computing Laboratory  
Electrical Engineering and Computer Science Department  
University of Michigan  
Ann Arbor, MI 48109-2122, USA  
farnam@eecs.umich.edu

### *Abstract*

Fault-tolerance in real-time systems is defined informally as the ability of the system to deliver correct results in a timely manner even in the presence of faults. Dependable real-time systems are being developed in diverse applications including avionics, air-traffic control, plant automation, automotive control, telephone switching, and automatic stock trading. These systems often operate under strict dependability and timing requirements that are imposed due to the interaction with the external environment. Meeting these requirements is complicated by the fact that a real-time system can fail not only because of software or hardware failures, but also because the system is unable to execute its critical functions in time.

This talk examines the interdependencies between real-time and fault-tolerance requirements, and presents various schemes for supporting redundancy while maintaining timing predictability. The talk also highlights operating system and communication support unique to the development of such systems. We draw upon examples from several distributed real-time systems including MARS, Totem, Delta-4 XPA, and ARMADA to illustrate these concepts. First, we will identify several distinguishing characteristics of real-time systems. We will discuss the distinction between hard and soft timing requirements, and highlight scheduling technologies to support real-time computing. Second, the problem of predictable redundancy management is considered.

In particular, we will examine passive and active replication schemes that provide fault-tolerance while maintaining timing predictability. We will also discuss how certain design methods effectively exploit accuracy( or quality of service ) as a third dimension to the traditional tradeoff between the time vs. space redundancy. Finally, system software to support the development of fault-tolerant real-time systems is described. We will identify requirements unique to such systems including operating system support, real-time communication, and clock synchronization.