# Systematic Composition of Real-Time Dependable Distributed Computing Systems

**Kane Kim**
UCI DREAM Lab
khkim@uci.edu
http://dream.eng.uci.edu/

For presentation at IFIP WG10.4 Meeting
Alyeska, Alaska
June 2008



# Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## A. Real-Time (RT) Distributed Computing (DC) Software Components

- **Components must be hard-RT components**
  - **This means there must be easily determinable hard bounds on the service times of the components.**
  - **Compositionality in the temporal dimension is then strong.**

- **Components must be powerful**
  - **in that all conceivable RT DC applications must be implementable as networks of components of the type and nothing else.**



## Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## A. Real-Time (RT) Distributed Computing (DC) Software Components

- **Components must be highly abstract (with no ambiguity embedded)**
  - **in that the mental effort required for designing and programming a component should be far less than that required for programming a construct that has equivalent computational effect and consists of threads, thread-priorities, and sockets.**
- **Components must incorporate a global time base**
  - **to enable TCoDA (Global-Time-based Coordination of Distributed computing Actions).**
- **Components must expose parallelism to a maximally practical extent.**





## Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## A. Real-Time (RT) Distributed Computing (DC) Software Components

- **Components must yield cost-effective methods for deriving tight service time bounds (STBs) of the components.**





# Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## B. Dependable Configurations of RT DC Components & Systems

- **Fault-tolerant (FT) configurations of components must yield tight bounds for recovery times**
  - **Recovery time here is defined as the service time increase due to failure occurrences**
  - **One could conceivably seek acceptable recovery time distributions rather than tight bounds but**
  - **Will it be really easy to produce credible, acceptable recovery time distributions when there is lack of deep insights into how to realize attractive tight bounds for recovery times ??**





## Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## B. Dependable Configurations of RT DC Components & Systs

- The less special hardware parts in the FT configurations the better off.
- Component replication schemes , cooperative fault detection schemes, and system reconfiguration schemes must be seamlessly integrated in cost-effective and analyzable forms.
- Access control and encryption mechanisms must be incorporated in harmonious forms into RT DC components.



# Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## C. Software Engineering Environments (SEEs) for Component-oriented RT DC Systems & FT Configurations

- **Given specifications on the fault types and rates to be concerned with,**

  **appropriate selection and tuning of fault tolerance mechanisms and configurations must be supported extensively by well-formed additions to SEEs for component-oriented RT DC systems.**





## Dreamer's View on Desirable Characteristics of a Composition Technology Sought

## C. SEEs for Component-oriented RT DC Systems & FT Configurations

- **Application-dependent parts of FT RT DC components and systems must be engineered under the support of well-formed SE tools.**





# Earlier Expectations & Current Status

## A. RT DC Software Components

- **Expectations in 20th Century**

  **Some reasonable component models will mature by 2000 – 2005.**

- **Status in 2008**

  **Nothing is mature &**
  **No major industry is pushing in recognizable forms.**

  – **Is the defense industry the only industry-segment that cares for it ?**





# Earlier Expectations & Current Status



- **TTP Programming Model**
  - **About the only effort being examined seriously by a major industry, i.e., automobile industry.**
  - **Based on combinations of statically scheduled tasks interacting via statically scheduled messages.**
  - **Compositionality is fine but the component model is viewed as a low-level model w.r.t. its use in a millisecond-level or coarser-grain timing-sensitive DC applications.**

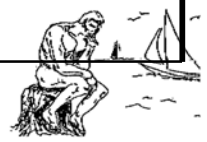


# Earlier Expectations & Current Status



- **Other serious efforts need at least 5 – 10 years to reach maturity.**

| | RT CORBA | RT Java | TMO |
|---|---|---|---|
| **Start** | 1996 | 1998 | 1992 |
| **Led by** | OMG SIGRT | SunMicro + A consortium + Academic Groups | Academic Groups + a small consortium |
| **Progress** | Version 1: Regarded as a failed approach<br><br>Version 1.2: Basic research phase | Cautious slow move – Not addressing DC cases yet.<br><br>Demos of single-node applications only. | Strong demos started appearing in 2004 (Remote Joystick, Digital Music Ensemble, MPVC, CAMIN--)<br><br>Taught to undergrads in UCI and a small number of other univs. |



# Earlier Expectations & Current Status

## B. Dependable Configurations of RT DC Components & Systems

- **Status in 2008**

  **Partly due to the slowness of the development of RT DC components, this technology area is getting delayed by 5 – 10 years from the original expectation.**

## C. SEEs for Component-oriented RT DC Systems & FT Configurations Status in 2008

- **Status in 2008 : Same as in B**





# Future Prospects

**Progresses are expected to be accelerated because**

- **Heightened international competition in realizing ubiquitous computing societies (which inevitably involve increasing numbers of safety-critical computing applications) and**
- **Computer systems and software technology researcher population in BRICs is still growing.**