Vanderbilt Workshop
New Visions for Software Design & Productivity:
Research & Applications
December 13-14, 2001
Vanderbilt University, Nashville, TN

(updated February 2003)
Motivating Examples

Contributor	Title	Description
Lockheed Martin (Joe Cross)	Verifiable Adaptability	We are developing the ability to design large, long-lived systems that adapt dynamically to changes in requirements (e.g., the ship enters battle mode, or a new function is added) and to changes in system components (e.g., damage, COTS refresh, or addition of new equipment). However, customers for mission-critical systems are unlikely to accept such system architectures until we are able to demonstrate, as early as design review time, that the deployed system will satisfy its requirements, before, after, and during adaptations. This presents two challenges. First, we must find system design methods that will yield verifiable designs, and second, we must find new ways to express requirements that are appropriate to adaptive systems (e.g., "maximum latency <= 1 ms" is probably not suitable.)
Lockheed Martin (Joe Cross)	Service Specification Language	It is now generally agreed (ref. OMG's MDA) that it is a mistake to build software components that are hard-wired to a single infrastructure (at least for long-lived components). E.g., a software component that works only with COM+ or CORBA is certain to need modification -- and possibly replacement -- within 10 years. An attractive alternative to hard-wiring to unique infrastructures is to design components that request named services, such as "point-to-point interprocess messaging". In general, specification of qualities of the requested service is also required, such as maximum latency of message delivery, or behavior when receive buffers are full. The challenge is to develop a taxonomy of requestable services, and a language for specifying the qualities of each service. This language would ideally be suitable for both system-build-time requests, when it would control the selection of alternative implementations of a given interface, and run-time requests, when it could control parameters of the executing service. Note that a mechanism such as this also requires a means to specify the loads that the components will impose on the services, such as rate and size distribution of messages, since without such data the quality of service that will be provided cannot be determined a priori.
Lockheed	Sharing Resouces	A common system architecture includes some critical stimulus-

Martin (Joe Cross)	between Analyzed and Un-Analyzed Threads	response threads which are subject to detailed analysis to ensure meeting critical requirements, and a large set of less critical threads which are not, and probably cannot be analyzed to the same level of detail. A critical threads should be able to share resources, including CPU and locks, with a non-critical thread. (The alternative is to dedicate resources to the critical thread -- i.e., a stovepipe.) The challenge is to design and implement systems such that the knowledge of the behavior of the critical threads is retained while sharing resources with threads whose behavior is largely unknown. This problem has presented itself starkly in Real-time Java, wherein it seems to be impossible for real-time and non-real-time threads to share a lock. One possible approach involves defining "breakable locks", where the cost of recovering a broken lock is paid by the non-critical thread that held the lock.
Boeing (Dave Sharp)	Design Time Challenges: Real-time modeling and analysis	Modeling characteristics and behaviors unique to real-time embedded systems remains a challenging research area, and one which is rarely used in practice or used in very limited ways. Lack of up-front analysis leads to large numbers of development iterations which are destined to be found unsatisfactory during testing. Lack of code generation technologies leads to each iteration requiring more effort than would be otherwise. Hurdles impeding progress include the cross-cutting nature of many embedded system characteristics (e.g. inherent coupling between distribution, scheduling, and fault tolerance), mismatch between theoretical assumptions and real-world systems (e.g. assuming atomic operations), and the predominance of proprietary architectures which limit open and widely applicable research. Advancement in these areas could reduce the number of development cycles, the cost of each, and confidence in the final product.
Boeing (Dave Sharp)	Design-Time Challenges: System dependability and certification	Even when applied to systems which during run-time are completely deterministic, productivity enhancement approaches associated with reusable component-based product line architectures surpass the capabilities of standard certification processes. Current certification approaches rely heavily on locally predictable and hard-code implementations. Product line approaches rely heavily on configurable components and late binding of characteristics during component integration. Reaping the benefits of component-based technologies in safety critical certified systems will require significant advances in certification techniques.
Boeing (Dave Sharp)	Run-Time Challenges: Multi-dimensional QoS Management	Managing and balancing the array of distributed real-time system characteristics in a manner that optimizes overall system performance is in its infancy. Adapting control systems based on changing physical plants (e.g. fuel burnt, payloads expended) and mission objectives (e.g. maximization of range, evasiveness, stealth) exceeds current capabilities. Adjusting computing resource utilization (e.g. CPU, bandwidth, memory) in the presence of changing mission modes (e.g. navigation, targeting, fire control) and external interfaces (e.g. sensor

		inputs) has been demonstrated only for relatively limited scopes (e.g. within a single CPU) and is rarely used in production. While it can greatly improve system effectiveness, it significantly complicates or invalidates current approaches to design time analysis and system certification.
BBN (Rick Schantz)	A Large Scale Information System Challenge - Focused Logistics: Precise Application of Logistics	Logistics Planning Challenges
Rockwell Collins (Gary Daugherty)	Specifying the Mode Logicof a Flight Guidance System in CoRE	Flight Guidance System
Rockwell Collins (Gary Daugherty)	CORBA Aircraft Example	Aircraft Example